PALGRAVE STUDIES IN FINANCIAL SERVICES TECHNOLOGY

BITCOIN AND MOBILE PAYMENTS

Constructing a European Union Framework

EDITED BY **GABRIELLA GIMIGLIANO**

Palgrave Studies in Financial Services Technology

Series Editor

Bernardo Nicoletti
University of Tor Vergata
Rome, Italy

The Palgrave Studies in Financial Services Technology series features original research from leading and emerging scholars on contemporary issues and developments in financial services technology. Falling into 4 broad categories: channels, payments, credit, and governance; topics covered include payments, mobile payments, trading and foreign transactions, big data, risk, compliance, and business intelligence to support consumer and commercial financial services. Covering all topics within the life cycle of financial services, from channels to risk management, from security to advanced applications, from information systems to automation, the series also covers the full range of sectors: retail banking, private banking, corporate banking, custody and brokerage, wholesale banking, and insurance companies. Titles within the series will be of value to both academics and those working in the management of financial services.

More information about this series at
http://www.springer.com/series/14627

Gabriella Gimigliano
Editor

Bitcoin and Mobile Payments

Constructing a European Union Framework

palgrave
macmillan

Editor
Gabriella Gimigliano
University of Siena
Italy

Palgrave Studies in Financial Services Technology
ISBN 978-1-137-57511-1 ISBN 978-1-137-57512-8 (eBook)
DOI 10.1057/978-1-137-57512-8

Library of Congress Control Number: 2016947653

Printed on acid-free paper

This Palgrave Macmillan imprint is published by Springer Nature
The registered company is Macmillan Publishers Ltd. London

Preface

Approaching Mobile Payments and the Bitcoin within the EU Framework: Rationale and Aims of the Study

Rationale of the Study

This Study investigates the regulatory issues of mobile payments (for brevity, m-payments) and virtual currencies, above all the Bitcoin. M-payments are devices for access to bank-based and non-bank-based payment systems, whereas virtual currency has been defined as a "digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money".[1] The Bitcoin, as a money like product, represents the most widespread decentralised virtual currency. Why then, if they work differently, are we developing them in parallel within the EU framework? In fact, there is a three-tiered rationale behind this choice.

Firstly, both enable prospective users to make online and offline purchases as well as to carry out customer-to-business, peer-to-peer and business-to-customer payments. Moreover, mobile devices may also allow holders to use Bitcoin currency through mobile wallets.

[1] ECB, Virtual currency schemes – a further analysis, February 2015, 25.

Furthermore, they are both ICT-based payment products and, as such, they play a critical role within the European strategy for a Digital Single Market.

The Digital Single Market plan aims to establish an area "where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or the place of residence".[2] To this end, the 2015 Commission Communication has set the following objectives: (i) to improve consumer and business access to online goods and services, (ii) to establish a suitable environment for the growth of digital networks and services, and lastly, (iii) to maximise investments in ICT infrastructures, research and innovation.

This is a long-lasting project whose roots may be traced back to Martin Bangemann's report on *Europe and the Global Information Society* produced for the European Council in 1994. Indeed, the Bangemann Report described the Western industrial model as a "perceived failure." This model was mainly based upon the heavy and automotive engineering and electronics industry, which had played an important role in the UK and German economic systems. On the other hand, the report concerned the information technology sector and took a liberal approach to technological development as guidelines for European growth.[3]

Accordingly, the 2000 Lisbon European Council, looking ahead to the next decade, set a new strategic objective of making Europe the "most competitive and dynamic knowledge-based economy in the world". This long-term strategy purported to remove the obstacles to cross-border online services and provide legal certainty for businesses, consumers or citizens. And for this, a flexible, technologically neutral legal framework was to be set up.[4]

---

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions, "A Digital Single Market for Europe", Brussels 6.5.2015, COM (2015) 192 final, 3.

[3] Philip Leith, "Europe's Information Society project and digital inclusion: universal service obligations or social solidarity?", *International Journal of Law and Information Technology* 20, no. 2 (2012): 102–123.

[4] Report from the Commission to the European Parliament, the Council and the Economic and Social Committee, Brussels. COM (2003) 702 final, 1–25.

Within this framework, the European Parliament and the Council passed, among other things, the e-commerce directive and, then, a couple of years later, the directive 2002/65/EC[5] on distance consumer contracts for the provision of financial services.

The e-commerce directive,[6] with its "internal market clause," enabled information society service providers to supply their services throughout the European Union according to the rules and regulations of the home Member State, while the 2002/65/EC directive set out a broad concept of financial services also covering payment services and provided a level of transparency at least comparable to that of the 97/7/EC[7] directive for financial service users in "distance" contracts.[8]

Under the 2002/65/EC directive, the customer has to be provided with a large amount of preliminary information. The duty of information covers the supplier and the financial service (main features, overall price, any additional costs charged, the arrangements for payment and the payment method, any special risks involved or the period of validity of the information and the distance contract itself) as well as the terms and conditions for exercising the right of withdrawal and out-of-court claim and redress systems.

The above-mentioned duties and obligations are laid down for the initial service agreement rather than the subsequent operations. This is the case for a bank account contract and for depositing operations. According to the preamble (17), opening a bank account or a contract to acquire a credit card are regarded as initial service agreements, while the act of depositing or withdrawing funds into or from a bank account (as well as a direct debit or a credit transfer order) are considered to be operations

[5] Directive 2002/65/EC of the European Parliament and of the Council of concerning the distance marketing of consumer financial services published in the OJEU of 9.10.2002 L271/16.

[6] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) of 8 June 2000 published on OJEC of 17.7.2000 L 178/1.

[7] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, published in *OJEC* of 4.06.1997 L 144, 19–27.

[8] Within the 2002/65/EC directive a contract was made "at a distance" when the offer, negotiation and conclusion took place via "means of distance communication". This was a technically-neutral idea and covered all the means of communication that work without the simultaneous physical presence of supplier and consumer.

coming under the initial service agreement and, as such, are neither imposed in the service provider disclosure and transparency duties nor do they grant the consumer the right of withdrawal.

When, in turn, the 2002/65/EC directive was amended by the 2007/64/EC directive (the so-called PSD), the harmonised framework for distance marketing of consumer payment services split up into two components; one general and the other special. The common field concerned the preliminary information to be provided to prospective customers. Thus, a prospective customer entering a distance contract must be provided with a set of preliminary information based upon the joint application of both directives.

According to the PSD, drawing the proper distinction between a framework contract for the provision of payment services and single payment transactions, the information to be provided covers: (i) the payment services provider, (ii) how the payment service works, (iii) all charges, interest and exchange rates, where applicable, to be paid by the user, (iv) the form of communication between user and provider, (v) the duties of the contracting parties, (vi) the user notification procedure in the event of changes to the contract, together with the termination regime and the duration of the contract, and finally, (vii) the redress system.

However, in compliance with the 2002/65/EC directive, when a means of distance communication is used and the contract is concluded at the request of the payment services user, this information may be provided immediately after the conclusion of the framework contract or immediately after the execution of the single payment transaction.

Despite the progress made, the 2012 Green Paper[9] considered payments to be one of the main barriers to the future growth of e-commerce. The regulatory concerns regarded the diversity of payment methods throughout the Member States, the cost of payments for businesses and consumers, and payment security issues.

Coming to the ultimate rationale behind this study, no dedicated framework has been laid down yet for either m-payments or the Bitcoin. While m-payments are subsumed under the general framework of the

[9] Green Paper "Towards an integrated European market for cards, Internet and mobile payments", Brussels, 11.1. 2012. COM (2011) 941 final, 3 ff.

2007 PSD and its update (PSD2) soon to be published officially, the Bitcoin, like other decentralised cryptocurrencies, seems to fall outside the community-based mainstream for payment services.

This wait-and-see approach sounds like something new in the European regulatory landscape. The last time the European lawmaker approached a new ICT payment product, namely e-money products, the European Parliament and the Council enacted two directives whereby issuing e-money was regarded as a regulated activity and the licensing and stability regime for e-money issuers was essentially shaped into the legislative framework for credit institutions.[10]

Indeed, the Commission contended that it was neither in the interest of the market nor that of the users for e-money to be distributed on an unregulated basis. So, in the opinion of the Commission, a legislative action was needed to ensure the soundness and stability of e-money service providers and, in the same way, the confidence of e-money bearers in this innovative means of payment. Accordingly, the Commission took a pro-active approach and drew up a double directive proposal.[11]

On the other hand, the European Central Bank endorsed the draft directive and proposed to incorporate the new e-money institutions within the umbrella of "credit institution" so as to impose reserve requirements and statistical reporting requirements. This was clearly stated in the opinion released during the legislative procedure. Here, the ECB argued that "this possibility (…) is crucial, in particular with the view to ensuring the preparation for a substantial growth in electronic money with a material impact of monetary policy."[12]

However, in the process of revising e-money directives, it was underlined how the growth of a "true single market for electronic money services" and the "development of such user-friendly services" have been hampered by some provisions of the 2000 e-money directives. In fact,

[10] Directives 2000/46 and 2000/28 of 18 September 2000 of the European Parliament and the Council on relating to the taking up and pursuit of the business of credit institutions, of 18 September 2000, published in OJEC L275 of 27.10.2000.

[11] Explanatory Memorandum. Commission Proposal for European Parliament and Council Directives on the taking up, pursuit and prudential supervision of the business of electronic money institutions.

[12] Opinion of ECB of 18 January 1999, OJ C 189 of 6 July 1999.

since the public consultation process, some critical remarks have been raised about the trade-off between restrictions on the object on the one hand, and the capital and own funds requirements on the other. In the end, a negligible number of community-based e-money institutions have received authorisation, namely the e-money institutions authorised to provide services throughout the Member States according to the principle of home country control and single licence. Only the 2009 directive on e-money institutions relaxed both the organization and stability requirements as well as restrictions on activity.[13]

Comparing the *ex ante* legislative strategy with the complete absence of a dedicated legal framework for m-payments and the Bitcoin, one might infer that neither of them represents a challenge to consumer protection or poses financial risks.

However, the international regulators' and supervision authorities' studies and surveys draw quite a different picture. It has been argued that m-payments and virtual currencies, especially the Bitcoin, can spur innovation and competition on the market for payment systems, but they may jeopardize financial integrity, fund safeguarding measures and the operation resiliency of payment networks.[14]

The point is that the "ecosystem" has become much more complicated. The stakeholders vary from inventors, miners and issuers to wallet providers, processing payment service providers, secure element issuers or mobile network operators. The presence of so many different stakeholders has not posed new types of risk, but has made the design and functioning of payment systems much more complicated, in addition to the regulation and implementation of security standards. In fact, open network communications and new business models may weaken the users' funds and data protection as well as heightening the risk of money laundering.[15]

---

[13] Directive 2009/110/EC of the EU Parliament and the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, published in OJEC L 267 of 10.10.2009, 7.

[14] Tanai Kiaonarong, "Oversight Issues in Mobile Payments", IMF Working Papers no. 123 (2014): 1–35; CPMI, "Non-banks in retail payments", BIS Publication, September (2014): 1–47.

[15] Terry Bradford, Fumiko Hayashi, Christian Hung, Simonetta Rosati, Richard J. Sullivan, Zhu Wang, and Stuart E. Weiner, "Nonbanks and Risk in Retail Payments: EU and U.S.", edited by M. Eric Jonhson, *Managing Information Risk and the Economics of Security* (Berlin: Springer 2009) 17–53.

Notwithstanding such regulatory concerns, the European Central Bank has recently looked into virtual currency schemes without producing an *ex ante* legislative strategy. It goes without saying that the Bitcoin, like e-money in the 2000s, may prove to be a threat to financial integrity, fund safeguarding and reduce payment system stability risks. However, this time, the ECB has refrained from proposing legislative action while there is still limited connection to the real economy and a low volume of Bitcoin being traded. To this end a careful monitoring activity will be put in place.[16]

In the end, whether m-payments and bitcoins may be used as valid tools for building up the Digital Single Market and the growth of e-commerce, as well as being a pro-competitive means for payment services on the market, it is essential to monitor their risks and drawbacks within the European Union framework.

Aims of the Study

As remarked in the previous paragraph, the European policymaker has refrained from laying down specific regulations for either of them. Given this background, the main issue to be addressed is a study of how the Bitcoin and m-payments on the one hand, and the EU rules and regulations on the other, interact.

The backbone of this analysis is naturally based on the EU law of payments, namely the PSD and PSD2[17] directive on payment services in the internal market and the 2009/110/EC directive. They lay down a comprehensive, but not exhaustive, framework for payment services and e-money products governing the professional provision of payment services and the issuance of e-money as regulated activities. Such directives have complementary goals, but they lay down a compulsory framework for consumers and micro-enterprises acting as users of payment services and holders of e-money. Indeed, they can enjoy

[16] ECB, "Virtual Currency Schemes – A further Analysis", February (2015).

[17] At this time, the PSD2 has not been approved yet.

– transparent economic and normative conditions for payment services, covering information before and after the operation of payment transactions;
– supervised payment service providers meeting stability and corporate organization requirements from the authorisation to the dissolution phase;
– basically homogeneous contracting duties and obligations for the provision of single payment services and payment account services.

Within this framework, the priority is to establish to what extent such a legal framework can be applied to m-payments and the Bitcoin, namely, to what extent m-payments and the Bitcoin can come under the concepts of payment service and e-money, at the heart of the regulatory and legislative backbone.

Furthermore, the study looks into a set of cross-sectorial regulatory concerns raised by payments using m-payments and the Bitcoin.

These cross-sectorial regulatory concerns can be placed in two groups:

– those covering the macro- and micro-economic issues common to every market and addressed by the international regulators and supervision authorities. They are based upon the participation of different service providers, the growth of non-financial providers and designing payment systems as open networks. Reference is made to anti-money laundering control, personal data protection and payment transaction security;
– the Europe-based issues, namely those essentially founded on the policy priorities of the European Union in terms of a Digital Single Market, a single area for payment and financial services, and a single area for European citizens, whether natural or legal persons. While the 2015 Commission Communication on a Digital Single Market saw different VAT regimes for cross-border e-commerce transactions as a legal burden, building up a level playing field among different payment service providers has always been a leading objective of the European Union. This has become much more challenging since telcos and mobile network operators are providing various value-added services so that voice, data and payment roaming activities are closely intertwined. In fact, antitrust and regulatory actions have been trading

off intra- and inter- system competition, applying the general principles of cartels and concentrations.

About this Book

In the light of the rationale and the objectives previously outlined, the book is an interdisciplinary volume looking into m-payments and virtual currencies, above all the Bitcoin, within the framework of the European Union, with a particular attention to comparative regulatory experiences.

To deal with this matter in the most comprehensive way, the volume is divided into four parts.

Part I deals with the "Institutional Strategies and Economic Background".

As already remarked, the EU policymaker is carrying out a long-term project to build up a single area for payment services. With regard to this project, Chap. 1 (by Gino Giambelluca and Paola Masi) analyses the regulatory trends in the EU framework within the field of innovative payments, and gives an overview of main policy priorities as well as the sources of law and regulators involved. On the other hand, Chap. 2 (by Gianni Bonaiuti) concentrates on a critical presentation of m-payments and the Bitcoin in economic terms. This sounds extremely important because not only is every regulatory action based on a reliable economic analysis but also the Court of Justice of the EU has long applied a functional approach to the enforcement of EU law.

Part II is devoted to "The Framework: a European and Comparative Outline". This part gives a legislative and regulatory analysis of m-payments and the Bitcoin blending the community-based and the comparative standpoints. Indeed, since there is no dedicated framework for m-payments and the Bitcoin, it is, nevertheless, much more important to investigate how the general European framework for payment and financial services covers the topic at issue. This study is carried out in Chaps. 3 and 4 (by Noah Vardi and Gabriella Gimigliano, respectively).

However, at the same time, the global nature of m-payments and the Bitcoin encourages scholars to go beyond the boundaries of the European Union, paying careful attention to third countries' legal systems and

well-qualified regulatory experiences. A comparative investigation is conducted in Chaps. 5 and 6 (by Andrea Borroni and Elisabetta Cervone, respectively).

Part III, on "The Challenges", concentrates on the leading regulatory challenges within the EU framework. They concern customers' funds and data integrity, the soundness of the payment and financial system, and the competitiveness of the European market.

The main topics covered are the policy priorities established by international regulators, European institutions and supervision authorities. In fact, Chaps. 7, 8, 9, 10 and 11 concern the security payment issues (by Safari Kasiyanto), personal data protection (by Gloria González Fuster), money laundering control (by Carolin Kaiser), VAT issues (by Redmar Wolf), respectively, and, finally, the operation of integrated business models within the EU competition framework (Daniele D'Alvia). All of them influence, to different degrees, the building-up process for a Digital Single Market and a single area for payment and financial services in the EU.

In Part IV, the "Conclusions", the final chapter by Benjamin Geva looks at the evolution of payment services and addresses continuity in diversity. As Professor Geva states, m-payments and the Bitcoin "(…) introduce new players in new roles and yet have not changed the basic architecture of the payment system."

Gabriella Gimigliano
Siena, Italy

References

ECB. (February 2015). Virtual currency schemes – a further analysis, Frankfurt am Main: European Central Bank. 1–37.

Bradford, T., et al. (2009). Nonbanks and risk in retail payments: EU and U.S. In M. E. Johnson (Ed.), *Managing information risk and the economics of security* (pp. 17–53). Berlin: Springer.

Kiaonarong, T. (2014). Oversight issues in mobile payments. *IMF Working Papers 123*, 1–35

CPMI. (2014). Non-banks in retail payments. *BIS Publication, September,* 1–47.
Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions. *A digital single market for Europe*. Brussels 6.5.2015, COM (2015) 192 final, pp. 1–20.
Leith, P. (2012). Europe's Information Society project and digital inclusion: Universal service obligations or social solidarity? *International Journal of Law and Information Technology, 20*(2), 102–123.
Green Paper. (2011). Towards an integrated European market for cards, internet and mobile payments. *Brussels*, 11.1. 2012. COM (941) final, pp. 1–25.
Report from the Commission to the European Parliament, the Council and the Economic and Social Committee Brussels. COM (2003) 702 final, pp. 1–25.

Acknowledgements

I am grateful to the European Commission Jean Monnet Programme, Education and Culture DG that sponsored my research granting the teaching module "Building up a Payment System for the European Union" of which this book is part. I must thank the University of Siena and, above all, the Department of Business and Law, for the accommodation of Jean Monnet project.

Contents

Contributors

Gianni Bonaiuti is Assistant Professor at the University of Siena where he teaches Monetary Economics. His research interests include topics on retail and wholesale payment systems, central banking theory and ECB monetary policy.

Andrea Borroni is a tenured researcher in Private Comparative Law at the Second University of Naples, Jean Monnet Department of Political Sciences. He was awarded a PhD by the University of Trento and an LLM with honors by the Louisiana State University (LSU) in 2006. He is currently teaching International Trade Law at the Second University of Naples, Jean Monnet Department of Political Sciences.

Elisabetta Cervone is Consulting Counsel at the World Bank, Finance and Markets Global Practice, Payment Systems Development Group. Elisabetta holds an LLM from George Washington University, USA. A Post-doctoral Fellow in Economics Law, University of Milan, a JD from University of Rome La Sapienza, and a PhD in Banking Law and Law of Financial Market at University of Siena, Italy. She is currently a Post-doctoral Research Fellow at the University of Milan, Italy.

Daniele D'Alvia is a Ronnie Warrington Scholar at Birkbeck University of London where he is a Lecturer in Comparative Law and in European Union Law. He has obtained several degrees (MA degree at the University of Rome "Tor Vergata", a Masters degree at "Il Sole 24 ORE" Business School, an LLM at Queen Mary University of London, and a GDL at BPP Law School). He is an

Italian qualified lawyer (*Avvocato*) and, *inter alia*, a fellow associate of the Higher Education Academy and a member of the Society of Legal Scholars.

Gabriella Gimigliano is a Law Graduate *cum laude* at Federico II University of Naples and holds a PhD in Banking Law and Law of Financial Market at University of Siena. She has been working as a Post-doctoral Fellow in Business Law and Economic Law and she is currently Lecturer in Business Law at University of Siena.

Gino Giambelluca has a Law degree and is a Co-Director of the Banca d'Italia, in the Market and Payment System Directorate. As a national expert, he contributed to various EU regulations in the field of payment services, on the Interchange Fee Regulation and the second Payment Services Directive. He is a member of the task force on payment services at the EBA (European Banking authority) and the ECB SecuRe Pay Forum.

Benjamin Geva is Professor of Law, Osgoode Hall Law School, York University and Counsel, Torys LLP, Toronto, Canada LLB (cum laude) (1970), Jerusalem; LLM and SJD Harvard Law School; Member of the Ontario Bar; Payment law international expert; Founding Editor of the *Banking and Finance Law Review*; and author of *Financing Consumer Sales and Product Defences*, *The Law of Electronic Funds Transfers*, *Bank Collections and Payment Transactions*, and *The Payment Order of Antiquity and the Middle Age*s and numerous articles.

Gloria González Fuster has a PhD, and is a Research Professor at the Vrije Universiteit Brussel (VUB), and also a member of the Law, Science, Technology and Society (LSTS) Research Group. She investigates legal issues related to fundamental rights, privacy, personal data protection and security, and lectures on fundamental rights protection in EU law. She currently participates in the research project *Promoting Integrity as an Integral Dimension of Excellence in Research* (PRINTEGER).

Carolin Kaiser LLM (mult.), is a PhD researcher at the Rijksuniversiteit Groningen in the Netherlands. She specializes in European technology and privacy law.

Safari Kasiyanto is a PhD researcher at Tilburg Law and Economic Centre (TILEC) and junior research fellow at European Banking Centre (EBC), Tilburg University, the Netherlands. He also works as a legal advisor at Bank Indonesia (the central bank of Republic of Indonesia); email address: S.kasiyanto@tilburguniversity.edu.

Paola Masi has a PhD in Economics from the University of Rome "la Sapienza", and is a principal manager in the Market and Payment System Directorate of Banca d'Italia. She is a member of the European System of Central Banks' working group on oversight on payment infrastructure and of the BIS oversight team for global payments and network providers.

Noah Vardi is Associate Professor of Private Comparative Law at the Law School of the University of Roma Tre, Rome, Italy. She is the author of a monograph on "The Integration of European Financial Markets: The regulation of monetary obligations" (Routledge, 2010).

Redmar Wolf has a PhD and is Senior Counsel with Baker & McKenzie Amsterdam and Professor of indirect taxes at the Faculty of Law of the VU University Amsterdam.

List of Boxes

List of Tables

Part I

Institutional Strategies and Economic Background

1

The Regulatory Machine: An Institutional Approach to Innovative Payments in Europe

Gino Giambelluca and Paola Masi

Abstract The authors deal with the evolution of the regulatory approach to innovative payments and describe the roles and actions of the authorities involved. The 2011 Green Paper "Towards an integrated European market for card, internet and mobile payments" sets out the first coherent European policy stance and priorities on e- and m-payments. Various initiatives have since been undertaken by the European Central Bank, the European Banking Authority and the European legislators especially in the field of security of payments, a key factor in enabling a sound growth of the new instruments. The final aim is to reflect on the adequacy of the present institutional architecture (division of powers, international cooperation, etc.) in fostering the development of an integrated, inclusive and competitive market of payment services.

Banca d'Italia. *Market and Payment System Oversight.* The opinions expressed do not necessarily reflect those of the Banca d'Italia.

G. Giambelluca • P. Masi (✉)
Banca d'Italia, Market and Payment Systems Oversight, Italy

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_1

Introduction

The evolution of the business models in the market for payment services constantly reflects a complex balance between regulation and technological progress. The diffusion of the internet and e-commerce, the development of mobile services and the new models of "service-sharing" economy entail electronic payment instruments that can be used anywhere, anytime, on the move or remotely, regardless of the location of the payer. The technology also continues to create opportunities for innovative business models, including mobile payments and virtual currency schemes.

In this context, the institutions and regulators are engaged in establishing rules and supervisory measures without hindering market developments; the operation is complex, due to the absence of geographical boundaries of the digital world. On top of this, there is the difficulty of synchronizing actions to technological developments and framing emergent phenomena, such as the virtual currency, with traditional legal and economic categories. One sign of this difficulty is the increased complexity of the institutional framework governing financial services and payment systems with increasing cross-sector and cross-border relations among supervisors. In Europe, discussion as to how to regulate innovative payment services is still underway, or better in intrinsic evolution, and might benefit from (i) the debate on innovation-friendly regulation; (ii) an overview of the recent institutional strategies for the development of innovative payments; (iii) an updated description of the framework, goals and tasks of the various authorities in the field, with the associated synergies and possible overlaps.

The Debate on an Innovation-Friendly Regulatory Environment

The economic debate on regulation, which is a central form of public intervention in the economy, usually considers it as either a driver for or a barrier to innovation. The very concept of regulation varies accord-

ing to the different historical and geographical context or the prevailing regulatory regimes. A broad definition includes formal tools (such as laws, regulations, directives, circulars, ordinances) and less formal ones such as market self-regulation and best practices (for example industry codes of conduct). The differences mainly reflect the way regulation is replacing other forms of public intervention, notably public enterprise or public-provided utilities.[1] Regulation affects incentives to innovate in various ways and interacts with phases of the innovation cycle, from R&D to commercialization.[2] The multi-tiered structure of legal sources and the allocation of regulatory powers among different institutions, at the national and/or cross-border level, tend to complicate the analyses.[3] The increasing globalization of economic activity and, in some currency areas, the blurring of the boundaries of the nation-state and nation-powers bring out the importance of the organizational perspective on the regulatory domain[4] which is a major element in building an innovation-friendly environment.

The financial industry is traditionally heavily regulated, also because its products are often the main or only instruments to finance innovation.[5] The impacts of financial rules on innovation have been treated under the more general analysis of the relation between regulation and economic growth and, specifically, in studies on the influence of competition and antitrust laws on capital investment.[6] The classical Schumpeterian approach under-

[1] Robert Baldwin, Scott Colin and Christopher Hood, Introduction to *A reader on Regulation*, eds. Robert Baldwin, Scott Colin and Christopher Hood (Oxford: Oxford University Press, 1998), pp. 1–58.

[2] Pelkmans, Jacques and Renda Andrea. "Does EU regulation hinder or stimulate innovation?." In Centre for European Policy Studies (CEPS), *Special Report* (Bruxelles: no. 96, November 2014), pp. 1–28.

[3] Enria, Andrea, "The Single Rulebook in banking: is it 'single' enough?" *in Lectio Magistralis* (Padova: University of Padova, 28 September 2015), pp. 1–2.

[4] Hancher, Leigh and Moran Michael, "Organising Regulatory Space" in *A reader on Regulation*, eds. Baldwin, Robert, Colin Scott and Hood Christopher (Oxford: Oxford University Press, 1998), pp. 148–172**.**

[5] Visco, Ignazio, Remarks in *Harnessing financial education to spur entrepreneurship and innovation*. 3rd OECD/GFLEC Global Policy Research Symposium to Advance Financial Literacy (Paris OECD 2015, May 7) pp. 1–5.

[6] Blind, Knut. "The Use of the Regulatory Framework to Innovation Policy" in *The Theory and Practice of Innovation Policy – An International Research Handbook*, eds Smits, Ruud, Shapira Philip and Kuhlmann Stefan (Cheltenham: Edward Elgar, 2010).

lines the negative impact of a (strong) competitive environment on the entrepreneur's willingness and ability to innovate: temporary monopolies, at the national and international level, might be an appropriate incentive to technological innovation.[7] By contrast, several empirical studies find a general positive influence of competition on innovation and economic growth.[8] Recent researches tend to seek a compromise between the diverging views: these studies recognize the complexities of the links between competition and innovation, focusing on their non-linear relation in a dynamic context and explicitly introducing plausible different influences of competition rules on the firm's incentive to innovate.

As for the payment infrastructures, the literature is still debating the opportunity to promote competition in clearing and settlement systems for financial transactions for two reasons in particular:

(i) they incorporate network effects with certain natural monopoly properties, like many utilities;
(ii) the main public interest in regulating payments sector is a matter of maintaining systemic stability (a question of risk allocation) and consumer protection.

However, many of the institutional reforms in payment systems, starting from the 2000 Cruickshank Report in UK and the Single Euro Payments Area (SEPA) project in the Eurosystem, were motivated by the need to increase competition, transparency, good governance, standards and fairness in the supply of payment services and infrastructures in order to promote innovative user-friendly (and rent-free) payments. As payment markets tend to be oligopolistic, regulators may try to open them up to new suppliers (as in the case of the non-banks and non-financial institutions in the EU) and to intervene in fee arrangements for an efficient redistribution of costs

[7] Aghion, Philippe, Akcigit Ufuk and Howitt Peter. "The Schumpeterian growth paradigm" in *Annual Review of Economics*, (Palo Alto, CA, 7 (2015) 557–575. Aghion, Philippe, Bloom, Nicholas, Blundell, Richard, Griffith, Rachel, and Howitt, Peter. "Competition and innovation: An inverted-U relationship" in *Quarterly Journal of Economics*, (Oxford, UK, 120(2) 2005): 701–728.

[8] Brandolini, Andrea and Ciapanna Emanuela. "L'ambigua relazione tra concorrenza e crescita." In *Concorrenza e crescita in Italia: il lungo periodo*, eds Gigliobianco, Alfredo and Toniolo Gianni (Venezia: Marsilio, forthcoming).

and revenues between various stakeholders. The tendency for regulators to place a stronger emphasis on payments efficiency, notably by tasking innovation,[9] has involved the government as a direct promoter of innovative payment services (for example by introducing new rules for electronic payments) and financial inclusion as a driver for innovative payment, using innovative payment instruments or low-cost new banking accounts to better integrate unbanked or underbanked people into the financial sector.

Together with the institutional reforms, the overall structure of regulatory framework (institutions, powers, standards, supervisory bodies, enforcements), and in particular how the dividing lines between and within regulatory entities are drawn, is influencing the effectiveness and costs of regulation for the economy and/or for sectorial economic agents.[10] The financial architecture is usually organized around three factors[11]: institutions, functions, and objectives. These three factors, not mutually exclusive, are usually combined to increase the resilience of the system. While regulation with an institutional focus addresses financial institutions irrespective of the mix of business undertaken, functional regulation takes the opposite approach. The design of regulatory structures, or the internal structure of a single regulator, is usually driven by the objectives of regulation: the ultimate criterion in devising its optimal structure should be the effectiveness and efficiency of regulation in meeting its basic objectives. The idea—shared and promoted by the international financial organizations—is that regulatory agencies are most effective and efficient, but also more transparent and accountable, when they have clearly defined, and precisely delineated, objectives and when their mandate is precise. However, when the objectives of regulation are potentially in conflict (for example promoting competition might

[9] Bank for International Settlements, *Innovation in retail payments.* (Basle: Committee on Payment and Settlement Systems, May 2012), pp. 1–58.

[10] Organisation for Economic Co-operation and Development (OECD). *The governance of regulators*. (Paris: OECD 2014) 13–28 and *Recommendation of the Council on Regulatory Policy and Governance.* (Paris: OECD, March 2012), pp. 3–19.

[11] Goodhart, Charles, Llewellyn David and Hartmann Philipp. "Reflections on Financial Regulation." in *Financial Stability Review*, (London: Bank of England, n.3 1997), pp. 51–60.

be in conflict with incentives to innovative services), one of the issues to consider is which structure is most efficient in resolving conflicts. In a single agency, for example, all conflicts are internalized. One merit of focusing institutional structure upon objectives is that it requires significant conflicts between such different objectives to be resolved at the political level, which does not necessarily correspond to optimal design of the overall financial architecture.

The Institutional Strategies for the Development of the Market for Innovative Payments

Over the past decade the European strategies for innovative payments have developed through a variety of interventions mainly related to three policy goals: promotion of greater competition between operators, integration of national markets into a single European area and enhancement of the security of payment systems and services. By following these three lines of policy we can arrive at a single and coherent overview of the latest regulatory developments in payment innovations.

Innovation and Competition

The first European directive on payment services (Directive CE/2007/64) focused on competition, by introducing a new category of payment service provider, the payment institution. With the hybrid figure of the payment institution, in particular, the aim of the legislator was to provide access to payment services to high-technological sectors enterprises (such as telecommunications); in fact, they were allowed to combine the supply of payment services with their traditional activities, taking advantage of their wide customer base and natural innovativeness. Although many years went by subsequent to the enactment of new rules, the goal was only partially achieved. The Telco world limited its interest in the payment industry, preferring business models that could enhance its specialization without changing the patterns of partnerships with the banking and financial sector

and without increasing the compliance costs. The Telco industry showed interest only in services not subjected to regulation, like those regarding the purchase of digital goods and services. In other words, the idea that mobile payment services debited on the phone bill could compete with traditional services offered by banks and card schemes, failed to find successful implementation. This is also why the new directive (PSD2), finally adopted by the European Parliament in October 2015, revised the scope of payment services that can be offered "without license" by telecommunications operators, based on a proportionate risk approach and with the aim to stimulate innovation. On one hand the legislator specified the categories of goods and services that can be purchased with phone bills, with explicit inclusion of donations and ticketing; on the other hand, it defined the maximum amount of waived transactions (50 EUR per transaction and 300 EUR monthly) so that operators wishing to handle larger flows must necessarily be licensed as payment institutions (see Box 1.1).

In comparison with the first directive, the PSD2 identifies additional business models in line with the strategy—affirmed by the EU Commission on several occasions—to encourage the development of a highly competitive market for e-payments. This strategy builds on the progressive and irreversible shift of trade and administrative relations to the internet (e-commerce, e-government) which, according to the community institutions, must be adequately supported with the development of efficient payment methods, easily accessible to all citizens also for cross-border transactions. In a market dominated by the use of payment cards on the internet, the legislator's intervention has developed along two lines: (i) revision of tariff rules and transparency in the world of card-based transactions, with the Interchange Fee Regulation (IFR), and (ii) formal recognition of the services enabling access to accounts, with PSD2. The two legal acts (PSD2 and IFR) build the frame for a safe and efficient use of payment instruments on the internet, fostering diversification of the means of payment available online and expanding the opportunities for e-commerce consumers and operators.

In terms of the impact on innovation, although many critics underline the risk of rapid obsolescence of the PSD2, the new regulation broadens the list of payment services with the inclusion of online services for the management of relevant information on clients—but with no financial

flows or management of funds—such as the initiation of the payment or access to account information. This acknowledges the ongoing changes in the approach to payment services by the financial industry: as in other innovative service models (e.g. crowdfunding or social lending), the management of customer information is relevant for access to the user's financial sphere (management of credentials, payment initiation and account balance information). Management of client information is becoming as relevant as the management of financial transactions for the reliability of the system.

Box 1.1 The Revised Payment Services Directive (PSD2)

The PSD2 updates the rules put in place by the Payment Services Directive (PSD) (2007/64/EC) which had the objective to contribute to a more integrated, secure and efficient European payments market, also improving the level playing field for payment service providers.

PSD2 widens the scope of the first directive by covering *new services and players.* In particular, new players have emerged in the area of internet payments offering consumers the possibility to pay instantly for their online shopping by a credit transfer, without the need for a credit card. These are the so-called "payment initiation services", which allow to establish a bridge between the payer's account and the online merchant, ensuring the latter that the credit transfer has been initiated and will be credited in the due time. Other services based on the access to the payment account are the "account information services" which allow consumers to have a global view on their financial situation and to analyse their spending patterns, expenses, financial needs in a user-friendly manner.

The new directive covers these new payment providers, until now not regulated at EU level, addressing issues which may arise with respect to confidentiality, liability or security of such transactions.

In addition to the exemption for payments for digital goods and services, PSD2 specifies the area of exemption for the *payment transactions through a commercial agent and the limited networks*. The exemption of the commercial agent is particularly relevant in the regulation of some e-commerce business models, as the online platforms and marketplaces, which will be deeply affected by the new perimeter of the waiver.

As mentioned in the "recitals", the exemption for commercial agent established in the first directive has been applied very differently in the Member States. Certain Member States allow the use of the exemption by e-commerce platforms that act as an intermediary on behalf of both

Box 1.1 (continued)

individual buyers and sellers without a real margin to negotiate or conclude the sale or purchase of goods or services. This implies risks for the consumers, as they are not covered by the protection of the legal framework, and also the effect of distortion of competition in the payment market. To address these concerns PSD2 clarifies that the exemption applies "when agents act on behalf of only the payer or only the payee, regardless whether being in the possession of clients' funds or not. Where agents act on behalf of both the payer and the payee (such as some e-commerce platforms), they might be exempted only if they do not enter at any time in possession or control of clients' funds."

PSD2 also revises the scope of the exception for payment services provided under a "limited network" or to buy a limited range of goods and services. The need to better define this exemption is related to the fact that it often involves significant payment volumes and values and it is exploited to pay for thousands of different products and services, with greater risks and no legal protection for consumers and disadvantages for regulated market actors. This is the reason why PSD2, also in recital, clarifies the conditions under which the exemption may be activated, introducing for the first time reporting obligations to the competent authorities and the European Banking Authority (EBA) over certain operating volumes, aimed at enhancing consumer protection and harmonized implementation of the waiver in Member States. As regards the consumers' rights, PSD2 provides a legislative basis to the unconditional refund right (within 8 weeks from when the payment is debited) that is already ensured by the pan-European direct debit scheme developed by the European Payments Council, fostering a higher level of consumer protection within the SEPA. In addition Member States may establish rules for refund rights that are more favourable to the payer. PSD2 also recognizes that the Member States may have the need to maintain legacy Euro-denominated direct debit, in order to address specific needs of the market, allowing that the payer and the payer's PSP agree in a framework contract that the payer has no right to a refund; this is possible when the payer gives consent to execute a transaction directly to his/her PSP and, where applicable, information on the future payment transaction was provided or made available to the payer for at least 4 weeks before the due date by the payment service provider or by the payee. In any case, the payer is always protected by the general refund rule, within 13 months after the debit date, in case of unauthorized or incorrectly executed payment transactions. Furthermore, the new directive increases consumer rights when sending transfers and money remittances outside the EU or paying in non-EU currencies. PSD2 will extend the application of the PSD rules on transparency to "one-leg transactions", hence covering payment transactions to persons outside the EU as regards the

(*continued*)

Box 1.1 (continued)

"EU part" of the transaction. As regards the fees and transparency rules, PSD2 discourages the practice of "surcharging" of the use of specific payment instruments (including debit and credit cards), both online and in shops. In all cases where card charges imposed on merchants are capped, in accordance with the regulation on interchange fees for card-based payment transactions (the IFR), merchants will no longer be allowed to surcharge consumers for using their payment card. This means the prohibition of surcharging for the 95 % of all card payments in the EU. As regards the regime of payment institutions, PSD2 largely confirms the licensing and operating requirements laid down by the current PSD. The main changes are related to the enhanced levels of payment security: entities that wish to be authorized as a payment institution shall provide with their application a security policy document, as well as a description of security incident management procedure and contingency procedures. Capital requirements which aim to ensure financial stability have largely remained the same under PSD2 as they were set out in the original PSD. Specific capital requirements have been defined for third party service providers in relation to their respective activities and the risks these represent. Third party service providers are not subject to own fund requirements. However, they need to hold a professional indemnity insurance covering the territories in which they offer services. PSD2 also enhances cooperation and information exchange between authorities in the context of authorization and supervision of payment institutions. The EBA develops a central register of authorized and registered payment institutions. As regards payment institutions that provide services cross-border, the supervision of these activities in principle remains with the home Member State, but the power of the host Member State has been reinforced; PSD2 has introduced better cooperation and information exchange between the national competent authorities during the passporting procedure. Furthermore, the host Member State can ask payment institutions operating with agents and branches in its territory to regularly report on their activities. In emergency situations, requiring immediate action, the host Member State is allowed to take precautionary measures with regard to the payment institution concerned, in parallel to the host's duties of cooperation with the home Member State to find a remedy. The PSD2 contains an option for Member States to require a payment institution that provides cross-border payment services to set up a central contact point if it operates with agents or branches that are established in their territory. The central contact point shall ensure adequate communication and information with regard to the activities of the payment institution in the host territory. The EBA is mandated to draft regulatory technical standards on the cooperation and information exchange between authorities and on the criteria under which a central contact point can be requested, and the functions of such contact point.

Innovation and Financial Integration: The SEPA Project

In Europe, the regulator supported innovation in payments industry also by creating an integrated payments market with EU Regulation 260/2012 which made the adoption of SEPA standards mandatory.[12] The harmonization of fund transfer methods can be an incentive for the development of innovative products and services that, based on the new SEPA circuit, may benefit from the reachability of payers and payees located in 34 different European countries. The SEPA credit transfer and the SEPA direct debit enable innovative payments in e-commerce, such as initiation of payment—regulated by PSD2, and new models of payment through mobile devices. In the latter field, an example is to be seen in the person-to-person payments (P2P) based on smartphones, which are gaining ground in several countries.[13]

The Euro Retail Payment Board (ERPB), which is the present governing body of the Eurosystem structural evolution in retail payments (see section "The ECB and the Eurosystem Role"), recently stated the need that "payment service providers offering P2P mobile payment services should make use of existing infrastructure as far as possible (for example SEPA payments and IBANs)."[14] Moreover, a harmonized process should be created to allow P2P mobile payment data (namely mobile phone numbers or email addresses and IBANs) to be exchanged between local solutions across borders": the ERPB therefore issued recommendations and set up a work-stream to identify standards to ensure full interoperability between existing solutions, based on the link between the archives

[12] After the introduction of the euro, disappointment with the state of cross-border integration for retail payments drove the European Commission to move actively in this field, having less confidence in a purely 'market-led' integration process (Ciani, Daniele and Masi, Paola. "Integration of EU Payment Systems: a 'tolerable straight line'?" in *Ianus Special Issue* 2014 (Siena: Università di Siena) 7–23).

[13] P2P mobile payments enable the exchange of funds in real-time person-to-person using a dedicated mobile app downloaded on the smartphone, functioning on the same basis as messaging services like '*whatsapp*'. The app generates a SEPA credit transfer between two accounts of the payer and the recipient which are associated with their respective telephone numbers.

[14] ERPB, *Statement*, 29 June 2015. https://www.ecb.europa.eu/paym/retpaym/shared/pdf/3rd_erpb_meeting_statement.pdf?6b0bc1dab8413a918607df831ad883df

containing IBAN codes and phone numbers managed by the providers of existing schemes.

P2P mobile payments enrich the mobile payments market and represent a good alternative to mobile payments based on wallet or payment cards, the most common in commercial transactions C2B. The impact on the market may prove highly significant: the reachability of all users in SEPA and the lower pricing model—if compared to card-based payments—make these services attractive for merchants, both traditional and online. Finally, it is worth noting that these kinds of services, even highly innovative, may benefit from the sound regulatory framework of the SEPA instruments.

Innovation and Security

The development of new business models and instruments also requires security. Even in the payments market, as in other sectors of the digital economy, the relationship between users and service providers is based on devices, applications and network infrastructure which operate most of the time outside the direct control of the parties in the financial relationship. Moreover, in the "sharing economy" model, the interposition is not only technological, but involves entire communities of users, who take on a direct role in the provision of services. In this context, we have a new form of confidence that underpins the commercial and financial relations between the parties which, given the level of complexity achieved, cannot be secured autonomously by any single actors in the digital market.

This is the reason why regulators have, in recent years, been activating measures that can help to reproduce in the digital environment the conditions for the development of strong relationships, based on full trust on interaction with purely virtual counterparts. For the first time, the PSD2, like other regulations in other sectors (see the NIS Directive), has intervened extensively on security issues, setting minimum requirements for payment services and providers. The new directive introduces rules both in the sphere of the customer, with the requirements for authentication of electronic payments and secure communication, and in the internal

organization of the payment service provider, where specific procedures are required in the licensing phase and in current operations.

Other measures have been introduced at the systemic level, such as the exchange of information between providers and competent authorities on significant security incidents.[15] This intervention is in line with the actions that global institutions are developing to enhance the security of critical sectors of the economy against the emergence of new malicious threats and vulnerabilities in the digital world; the definition of an effective "cyber security strategy" at national and European level, is one of the pillars for the creation of the European "digital single market",[16] of which the financial services and payment industry are an essential component. As part of this framework, the PSD2 is aiming at defining a set of clear rules for the services of the digital world and a new sphere of rights and protections for its users.[17]

The Role of the Authorities

The present institutional framework in charge of setting out the rules and supervision on the European and international payment systems is very complex. The competent national authorities and various supranational institutions, with different skills and tasks, play a role in guiding and promoting the development of the sector. Indeed, the growing complexity of the European institutional machine is reflected also in the area of payments, in which the main players are the European Commission, the EBA and the Eurosystem.

---

[15] As declared in the PSD2 "recitals" it is essential that payment service providers report major security incidents "in order to ensure that damages to other payment service providers and payment systems, such as a substantial disruption of a payment system, and to users, is kept to a minimum".

[16] European Commission, *A Digital Single Market Strategy for Europe*, (Bruxelles: COM(2015)192), 6 May 2015.

[17] Other major pillars of the framework are Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014 and EU General Data Protection Regulation (currently in the final stage of approval).

The EU Commission

In recent years, the EU legislator (Parliament, Commission and European Council) has focused its action in integrating retail payments in the single market through the development of a comprehensive legal framework for payment services and electronic money on the basis of: Directive 2007/64/EC on payment services, Regulation (EC) No 924/2009 on cross-border payments in the community**,** the E-money Directive 2009/110/EC, the SEPA Regulation No 260/2012 and, lastly, the Regulation of interchange fees for card-based transactions No 2015/751 and the revised Directive on payment services.

The legislative action has been able to rely on the support of various impact studies and consultative reports. The 2011 Commission Green Paper "Towards an integrated European market for card, internet and mobile payments" is still an important reference since it sets out the principles and objectives for the development of an efficient and competitive market for innovative payments. From the regulatory point of view, the need to intervene is still justified by the persistent fragmentation of important areas of the payments market, in particular card payments, along national borders and by the lack of consumer protection and security in certain areas, e.g. internet and mobile payments. Development of an integrated single market for safe electronic payments "is crucial in order to support the growth of the Union economy and to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to fully benefit from the internal market."[18]

To keep dialogue open with the Member States on these issues, the Commission relies on dedicated bodies and working groups[19] with the task to foster harmonization in the transposition and implementation of the EU legal framework. The need for a permanent monitoring of

[18] PSD2 "recital", no. 4.

[19] The two main examples are the *Payment Committee* and the *Expert Group on Banking*, *Payments and Insurance*, created after the entry into force in 2009 of the Treaty of Lisbon. The two committees support the delegation of executive powers to the European Commission, provide advice/expertise in the area of payments and assist the Commission in the preparation of Implementing Acts and Delegated Acts of each regulation.

payment innovations also reflects the difficulties of the EU regulator in framing payments market: the strong competitive pressures of international players, the speed of technological change, the ability to take advantage of the more favourable regulations, the complex and difficult process for setting standards are all factors that affect the effectiveness of traditional instruments of controls. Different forms of dialogue with the market and among national competent authorities are also needed to ensure consistency and effectiveness in the application of rules throughout the EU Member States.

The EU Commission's reliance on technical studies, working groups and direct involvement of competent authorities, self-regulated organizations (SRO) and market operators in the regulatory process is growing with the growth of the single market. Given the difficulties in finding appropriate incentive for new payments and remaining neutral towards the different business models, the Commission's approach entails the risks of over-regulating the sector and overlapping with the actions and proposals of other authorities. This might increase the perception of possible inefficiencies in the EU distribution of regulatory powers.

The European Banking Authority

The EBA is emerging as an important actor in the institutional framework for payment services. In line with the assigned mandate—set by law (Reg. no. 1093/2010)—to contribute to the stability and effectiveness of the financial system, the EBA has recently been taking a greater interest in the payment market, since its functioning is relevant to many of EBA's objectives, like promoting a level playing field for competition, ensuring that risk taking is appropriately regulated and supervised, and enhancing customer protection. The EBA is mandated to monitor new and existing financial activities and adopt guidelines and recommendations, with a focus also on innovations.

In July 2014, based on a thorough study of the phenomenon, the EBA issued an *Opinion on Virtual Currencies*, setting out a regulatory approach towards this particular innovation and inviting the European institutions

to regulate it.[20] The EBA suggests intervening on those entities that offer conversion services between virtual and legal currencies (virtual currencies exchangers) by including them within the scope of application of the anti-money laundering legislation[21]; finally, the EBA invited the supervisory authorities of Member States to discourage banks, electronic money institutions and payment institutions from engaging in operations related to virtual currencies, pending the issuance of the regulation. The risk profile of virtual currencies has been addressed by several other international regulators, such as the Financial Action Task Force (FATF) (Box 1.2).

Another important step in the EBA's work on innovative payment services came with publication of the Guidelines on the Security of Internet Payments in December 2014. Being based on the European Central Bank (ECB) Secure Pay Recommendations, the guidelines represent a good example of cooperation between institutions in addressing the new challenges of the payment market. In 2015 the EU legislator acknowledged the importance of the EBA's role in the payment systems and its cooperation with the Eurosystem, conferring upon it a series of mandates to develop regulatory technical standards and guidelines, especially on security issues.[22]

[20] The possibility to include regulation of virtual currencies in PSD2 was excluded during the negotiation of the directive PSD2; a new opportunity could arise with the next update of the directive on electronic money.

[21] As part of the proposal of the Directive on the prevention on the use of the financial system for the purpose of money laundering and terrorist financing (AMLD4). According to the Committee on Payment and Market Infrastructures (CPMI, *Report on Digital Currencies* (Basle: CPMI November 2015)), the borderless online nature of digital currencies and the absence of an identifiable "issuer" of the instrument have raised important concerns by law enforcement authorities about the use of these systems and currencies for illegal activity, as well as compliance with AML/CFT obligations that apply to traditional payment methods and intermediation.

[22] The reference is to the Interchange Fee Regulation (IFR), which requires the EBA to develop Regulatory Technical Standards (RTS) to ensure separation between card schemes and processing entities, and to the revised Payment Services Directive (PSD2), which confer on the EBA the task of developing six Technical Standards and five sets of Guidelines. In accordance with the procedure laid down in Article 15 of Regulation (EU) No 1093/2010, the technical standards are formally adopted by the EU Commission.

Box 1.2 The FATF Guidance

In June 2014, the FATF issued the report *Virtual Currencies Key Definitions and Potential AML/CFT Risks*. Despite the benefits of payment and financial innovation, the FATF underlines that virtual currencies' payment products and services (VCPPS) present money laundering and terrorist financing (ML/TF) risks and other crime risks that must be identified and mitigated. To this end the FATF issued a *Guidance for risk based approach (RBA) to virtual currencies* (June 2015) which focuses on applying the risk based approach to the ML/TF risks associated with VCPPS.

The Guidance is dividing virtual currency into two basic types: *convertible* and *non-convertible* virtual currency. The notion of "convertible currency" does not in any way imply an ex officio convertibility (e.g. in the case of gold standard), but rather a de facto convertibility (e.g. because a market exists). Thus, a virtual currency is "convertible" only as long as some private participants make offers and others accept them and has an equivalent value in real currency and can be exchanged back and forth for real currency. The Guidance is on the points of intersection ("nodes") that provide gateways to the regulated financial system, in particular "convertible virtual currency exchangers" in order to clarify the application of the relevant FATF recommendations to them.

Convertible virtual currencies may be either of two sub-types: *centralized* or *decentralized. Centralized* virtual currencies have a single administrating authority (administrator)—i.e. a third party that controls the system. An administrator issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation). The exchange rate for a convertible virtual currency may be either floating—i.e. determined by market supply and demand for the virtual currency—or pegged—i.e. fixed by the administrator at a set value measured in currency or another real-world store of value, such as gold or a basket of currencies. Currently, the vast majority of virtual currency payments transactions involve *centralized* virtual currencies (examples: Second Life "Linden dollars"; PerfectMoney; WebMoney "WM units"; World of Warcraft gold). *Decentralized* virtual currencies (or cryptocurrencies) are distributed, open-source, math-based, peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight (examples: Bitcoin; LiteCoin; Ripple).

Convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering and terrorist financing abuse for many reasons. First, they may allow greater anonymity than traditional non-cash payment methods. Virtual currency systems can be traded on the internet, are generally characterized by non-face-to-face customer relationships, and may permit anonymous funding.

(*continued*)

Box 1.2 (continued)

Decentralized systems are particularly vulnerable to anonymity risks. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems.

Virtual currency's global reach likewise increases its potential AML/CFT risks. Virtual currency systems can be accessed via the internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of *decentralized* virtual currency technology and business models, including the changing number and types/roles of participants providing services in virtual currency payments systems. And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls.

The ECB and the Eurosystem Role

Given its mandate to streamline the operation of payment systems, the Eurosystem has always had a strong interest in promoting innovation in payment system. The ECB and the national central banks played a fundamental role in the migration of the European banking community to the SEPA, as it was considered the natural step following upon the introduction of euro banknotes and coins. According to the EU Treaty, efficiency and reliability are the main drivers of the Eurosystem activities. Through its oversight function, the Eurosystem carries out assessments of the safety and efficiency of payment systems, payment schemes and instruments; it has also worked to promote a common understanding on security issues by setting up a European forum on the security of retail payments known

as "SecuRe Pay Forum", with the participation of representatives from banking supervision and oversight. The SecuRe Pay Forum has formulated recommendations for security of internet and mobile payments that, despite the lack of enforcement on the basis of the regulatory framework in place, have been taken into consideration for the issue of EBA guidelines on internet payments and represented the starting point of the primary PSD2 rules regarding security of payments (see Box 1.3).

Box 1.3 The EBA Guidelines on the Security of Internet Payments

In the light of the growth of frauds registered on internet payments (794 million euro in fraud losses in 2012, up by 21.2 % from the previous year), which undermine the confidence of market participants in payment systems, EBA decided at the end of 2014 to publish the guidelines on internet payments, based on the content of ECB Secure Pay Recommendations, with the implementation date of 1 August 2015.

The purpose of the guidelines is to define common minimum requirements for the internet payment services, such as: the execution of card payments on the internet, including virtual card payments; the registration of card payment data for use in 'wallet solutions'; the execution of credit transfers on the internet; the issuance and amendment of direct debit electronic mandates; transfers of electronic money between two e-money accounts via the internet.

The guidelines, in addition to the requirements, also provide a set of best practices which payment service providers are encouraged, but not obliged, to follow.

Mobile payments—other than those browser-based—are excluded from the scope of the guidelines, together with payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology and payment transactions made by an enterprise via dedicated networks.

The guidelines provide for requirements related to three different areas:

1. *General controls and security environment*; payment service providers are requested to implement and regularly review a formal security policy for internet payment services. They should carry out and document thorough risk assessments with regard to the security of internet payments and related services, both prior to establishing the services and regularly thereafter. Payment service providers should ensure the consistent and integrated monitoring, handling and follow-up of security incidents; they have to establish a procedure for reporting

(*continued*)

Box 1.3 (continued)

such incidents to management and, in the event of major payment security incidents, the competent authorities. Payment service providers should implement security measures in line with their respective security policies in order to mitigate identified risks. They must have processes in place ensuring that all transactions, as well as the e-mandate process flow, are appropriately traced.

2. *Specific control and security measures for internet payments*; the most important rules in this area are those related to strong customer authentication, which is required for the initiation of internet payments, as well as for actions which imply high risks for the customer, as the issuance or amendment of electronic direct debit mandates or the access to or amending of sensitive payment data. Alternative measures may be adopted in some pre-identified categories of low-risk transactions, based on a transaction risk analysis or involving low-value payments, as referred to in the PSD. Also providers of wallet solutions are requested to support strong customer authentication when customers log in to the wallet payment services or carry out card transactions via the internet. Other requirements are applicable to the process of customer enrolment, the provision of authentication tools or software delivered to the customer, and the transaction monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions.
3. *Customer awareness, education, and communication;* the guidelines require the payment service providers to offer assistance and guidance to customers with regard to the secure use of the internet payment services; they also have to provide at least one secure channel for ongoing communication with customers regarding the correct and secure use of the internet payment service. The payment service providers should explain the procedure for customers to report the suspected fraudulent payments, suspicious incidents or anomalies during the internet payment services session and/or possible social engineering attempts. Payment service providers have to set limits for internet payment services and provide their customers with options for further risk limitation within these limits. They may also provide alert and customer profile management services, including the confirmation of the payment initiation and the information necessary to check that a payment transaction has been correctly initiated and/or executed.

As mentioned before, PSD2 introduces a wider set of security requirements for payment service providers: even if many of them are completely new, due to the need to cover the emerging risks related to the business model of the digital economy, a number of provisions are fully in line with the framework of security requirement designed by the EBA and, even before, by the ECB Secure Pay Recommendations.

The Eurosystem also performs a less formal role as catalyst, providing guidance and support to the payments industry and other stakeholders in the development of common standards, interoperability rules and cooperative actions which may foster innovation and efficiency in all the segments of the payment chain. This includes a wide range of activities, such as issue of reports, organization of seminars and conferences for market operators and the creation of fora for discussion, at the national and European level. A major step forward in this role was the establishment in 2015 of the Euro Retail Payments Board, a new entity established and chaired by the ECB with the aim to foster a continuous dialogue with the stakeholders for the development of an integrated, innovative and competitive market for retail payments in euros in the European Union.

As stated in its mandate,[23] the ERPB is composed of representatives of both the supply side (payment service providers) and the demand side of the market (consumers, retailers, and corporates and public administrations). The ERPB's work will consist mainly in formulating common policy stance, guidance, statements and strategic views on the needs of the payment service market; its main task is to identify key issues and work priorities (including business practices, requirements and standards) and to ensure that they are addressed. In the first year of its life, ERPB addressed various issues relevant to the field of innovation, such as the instant payments, P2P mobile payments, e-invoicing, where there is a need to find the right balance between integration and the promotion of a sustainable level of competition.

Conclusions

In recent years the European payment systems, services and products have been heavily regulated. The general objective to complete European integration has led the primary legislator to impose detailed

[23] https://www.ecb.europa.eu/paym/retpaym/shared/pdf/ERPB_mandate.pdf. On the supply side of the market, there participate four representatives of the banking community, two representatives of payment institutions and one representative of e-money institutions; on the demand side of the market, two representatives of consumers and one representative of each of the following stakeholder categories: (i) retailers with a physical presence, (ii) internet retailers, (iii) businesses/corporates, (iv) small and medium-sized enterprises and (v) national public administrations.

technical requirements for payment instruments (the SEPA project) to remedy failures in coordination among market operators; moreover, the goal of opening the market up to competition and avoiding unfair differences in sharing the regulatory burden among specific business models led to more closely detailed regulation. The usual criticisms of these type of regulatory interventions underline the high risk of inconsistencies with the speed of technological and market changes and with an innovation-friendly regulatory approach, which would require flexibility and neutrality towards the various market business models and products. In this perspective, the role of the secondary regulations developed by specialized institutions in banking and financial matters, such as the EBA, can be better suited to increase effectiveness and promptness of response in regulators' action. In the same line, by promoting the dialogue with all the stakeholders and operators in new bodies, such as ERPB, it may be possible to combine innovation with interoperable and competitive system solutions and the development of new security standards.

Effective regulation of emerging phenomena, such as the virtual currency or m-payments, requires technological neutrality, clear definition of objectives of the various authorities/bodies involved, and institutional standardization fora. On payment innovation, more than in other fields, the regulators' approaches and actions should be driven more by the results of the dialogue among interested bodies or economic agents than by the mere dynamics of "market forces". Awareness of and transparency in the main public interests behind any new financial innovation can help to design a proper regulatory framework, despite the growing institutional complexity, the potentially inefficient allocation of regulatory powers and the global dimension of market agents.

References

Aghion, P., Nicholas, B., Richard, B., Rachel, G., & Peter, H. (2005). Competition and innovation: An inverted-U relationship. *Quarterly Journal of Economics, 120*(2), 701–728.

Aghion, P., Ufuk, A., & Peter, H. (2015). The Schumpeterian growth paradigm. *Annual Review of Economics, 7*, 557–575.

Baldwin, R., Scott, C., & Christopher, H. (Eds.) (1998). *A reader on regulation*. Oxford: Oxford University Press.

Bank of International Settlement. (2012, May). *Innovation in retail payments.* Basle: Committee on Payment and Settlement Systems.

Blind, K. (2010). The use of the regulatory framework to innovation policy. In S. Ruud, S. Philip, & K. Stefan (Eds.), *The theory and practice of innovation policy – An international research handbook*. Cheltenham: Edward Elgar.

Brandolini, A., & Emanuela, C. (forthcoming). L'ambigua relazione tra concorrenza e crescita. In A. Gigliobianco & T. Gianni (Eds.), *Concorrenza e crescita in Italia: il lungo periodo*. Venezia: Marsilio.

Ciani, D., & Masi, P. (2014). Integration of EU payment systems: A 'tolerable straight line'? *Ianus Special Issue. Modulo Jean Monnet*, 7–23.

Committee on Payment and Market Infrastructures (CPMI). (2015, November). *Report on digital currencies.* Basle: CPMI.

Enria, A. (2015, September 28). The single rulebook in banking: Is it 'single' enough? In *Lectio Magistralis.* Padova: University of Padova.

Financial Action Task Force (FATF). (2014, June). *Virtual currencies key definitions and potential AML/CFT risks.* Paris: OECD

Financial Action Task Force (FATF). (2015, June). *Guidance for risk based approach* (*RBA*) *to virtual currencies.* Paris: OECD

Goodhart, C., David, L., & Philipp, H. (1997). Reflections on financial regulation. *Financial Stability Review*, London: Bank of England, *3*, 51–60.

Hancher, L., & Michael, M. (1998). Organising regulatory space. In R. Baldwin, C. Scott, & C. Hood (Eds.), *A reader on regulation*. Oxford: Oxford University Press.

OECD. (2012, March). *Recommendation of the council on regulatory policy and governance.* Paris: OECD.

Organisation for Economic Co-operation and Development (OECD). (2014). *The governance of regulators*. Paris: OECD.

Pelkmans, J., & Andrea, R. (2014, November). *Does EU regulation hinder or stimulate innovation?* Centre for European Policy Studies (CEPS), Special Report, CEPS No. 96, Bruxelles.

Visco, I. (2015, May 7). Remarks, harnessing financial education to spur entrepreneurship and innovation. In *3rd OECD/GFLEC Global Policy Research Symposium to Advance Financial Literacy*. Paris: OECD.

2

Economic Issues on M-Payments and Bitcoin

Gianni Bonaiuti

Abstract Technology innovation and new consumers' habits are fostering two interesting experiences in the payments' landscape: the increasing use of mobile payment instruments and the emergence of alternative payment schemes without fiat or banking money, like Bitcoin. This contribution considers both cases as useful drivers for innovation, but at present their positive outcomes are unclear. A synthetic economic analysis highlights costs and benefits for consumers and third-party operators, arguing that mobile payments could improve competition and force banks to rethink their strategies. More controversial issues concern bitcoin: on this topic enthusiastic expectations of financial operators are jointly considered with cautious positions expressed by regulatory and monetary authorities. Recent tendencies in Bitcoin's informal infrastructure are confirming that an effective decentralized and peer-to-peer payments system is rather hard to build.

G. Bonaiuti (✉)
Assistant Professor, University of Siena, Italy.

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_2

Introduction

In recent years there has been an improved attention towards payment system: many contributions have focused on two relevant topics considered as drivers of future change in this sector: the increasing extension of the mobile payments and the flourishing of experiences where people use the so-called virtual currencies, bitcoin being the most known and disputed one. From an economic viewpoint, the two cases are obviously different, but they are gathered by important factors like technological innovation and increasing transactions on the internet. Mobile payments can foster new payment instruments and procedures, that could compete and probably prevail on the existing ones, provided by banking operators, whose strategies are not yet defined; this raises little concern on possible influence on monetary control, even if this scenario is not at hand, despite that mobile payments are expected to grow at a very high rate in the future.

As occurred in the past, the birth of new products or services characterized by network externalities puts in motion a preliminary process for strengthening a standardized model of payments operations, which is necessary to reach the critical mass allowing competitive mutual interchange of instruments (interoperability) and correlated benefits for users. At present, this is not the case, since none of the many market solutions in mobile payments has yet achieved the market share necessary to convert it into a standard. As is well known, both sides of the retail payment market are mutually dependent: the supply of a new product is scarce if demand appears to be slow, but, symmetrically, demand cannot expand without adequate offer conditions. At the initial stage users have to choose between many non-compatible products, while providers need an adequate level of demand to compensate for the required expensive fixed investment.

The second topic has wider implications, for the potential threat that it poses to the stability of existing monetary function and institutions, whose systemic consequences are currently unclear. As many contributors state, the Bitcoin scheme constitutes an example of an alternative monetary function (including money) completely separated from public institutions (central bank or government) and free from traditional third

parties, such as banks or other intermediaries. A decentralized payment scheme, especially for small amount transactions, could bring advantages of cost reduction and ease of use. According to others, the bitcoin experience will deploy its effects far beyond global transfer of funds: its core innovation is the public ledger of all the executed transactions that could be applied to other activities implying registered property transfers. Its adoption would produce accuracy of single operations without regulatory intervention.

Some doubts could be raised about a structure based on voluntary contributions without any central body of coordination: to promote bitcoin's acceptance as a medium of exchange, a coordination team should be established, even at minimum level of complexity, just to provide the correct information needed to enter the scheme. Instead, and in conflict with the original peer-to-peer approach, currently we observe a concentration process that exploits scale economies in a particular and essential phase of the process, that of mining, which is the creation of additional units of the new money.

Even if both mobile payments and virtual currencies constitute an important outcome of progresses in information technology, they require separate analysis: the expected growth of the first will produce changes in an existing framework, while the extension of the second might pave the way for an entirely new payment environment.

It is hard to predict all the possible outcomes that a new payment procedure can support: historically there have been many examples of innovative instruments, not fostered by market tendencies; two decades ago, e-money was considered a substitute of all traditional money and its expected fast growth a potential damage for central banking. Conversely, other past experiences of money privately issued have confirmed that an essential function like the monetary one, cannot be carried out under private incentives scheme in a completely unregulated manner, due to its public interest nature.

While mobile payments are compatible with existing "traditional" money (fiat money and banking sight deposits), schemes based on the so-called "virtual currencies"—like the Bitcoin scheme—constitute an alternative because a virtual currency is functionally separated from prepaid cards or bank accounts. The economic issues that they open up regard

micro and macro aspects: first of all we have to consider the eventual benefits accruing to consumers and intermediaries (cost reduction); secondly, attention must be paid to systemic aspects. In particular, the lack of regulation could increase the negative spillover effects on the payment system when a loss of confidence occurs.

Issues on Mobile Payments

According to the definition expressed in a recent document by the European Commission,[1] a mobile payment is payment for which data and instructions are initiated and confirmed by mobile device, so focusing attention more on procedures than on payment instruments or mediums of exchange. Mobile payments can enter a card scheme (credit or debit card) and produce a final transfer of money using bank accounts, as usually required in internet-based transactions. This clarification confirms the overlapping of three separate concepts: instrument, procedure and money, but their distinction will be less evident in the future, mainly between mobile and electronic payments.[2] Separate issues concern users and providers of mobile payments: usually the propensity to use one form of payment depends on basic features like saving on cost and time, beyond convenience of use. This is a rational choice when alternatives exist; in other words, mobile payments have to provide at least the same access conditions provided by traditional payment procedures, like card-based schemes.

Two categories of m-payments exist: proximity and remote payments.[3]The first one requires a specific mobile device enabled to near field communication (NFC) technology—a protocol to transfer data on

[1] European Commission, *Towards an integrated European market for cards*, *internet and mobile payments*, Green Paper, Brussels, 11 January 2012.

[2] According to European Commission, *Towards an integrated European market for cards*, *internet and mobile payments*, Green Paper, Brussels, 11 January 2012, e-payments are payments made over the internet via remote payment card transaction, or online banking procedures, or trough e-payment providers.

[3] The European Central Bank, *Recommendations for the security of mobile payments*, Frankfurt, November 2013 adds to these a third category of m-payments, when executed via MNO services, without using a specific application installed on mobile device.

a very short distance—and a terminal located at the point of sale. In such a way, a mobile payment operates like a contactless card and its use is convenient where payment is forced to a specific location, as in public transport services or car parking. Using a NFC smartphone, consumer uses the "physical" point of interaction (POI) available in the brick-and-mortar merchant's shop,[4] making a wireless connection and executing payment: an application installed in the personal device starts the procedure, then is completed by the merchant's service provider.

Remote payments are a more interesting case since its use is not constrained by any specific point of access, thus being a "molecular grid" of access points that make easier the act of payment as if one spent cash. The advantage of remote payments lies in facilitating both procedures and instruments of payment: theoretically all traditional payment instruments (cards, credit transfers, directs debits) could be used via a remote mobile scheme, simply by a dedicated software application installed on a smartphone.[5] In the proximity payments too procedures are launched by a smartphone application, but in a more complex manner: communication between users and merchants requires web access to the merchant's website and obviously it has to be done everywhere; following the purchase of goods and services, like a traditional e-commerce transaction the payment procedure involves the payment gateway as the third component. The latter acts as controller and communication service, separated from the e-commerce website. In the remote mobile payments too the merchant's payment service provider is engaged: its duty is managing funds' transfer originated by the transaction. With regard to the European Union, to execute a mobile payment, proximity or remote, both payer and beneficiary have to own a SEPA code payment account or a SEPA compliant card, through which funds will be transferred[6]; the application in the mobile device selects instruments and procedures according to the

[4] For a detailed analysis European Payment Council, *White paper Mobile wallet payments*, January 2014.

[5] Mobile payments applications are different from online banking services accessed by remote devices. See European Payment Council, *White Paper Mobile Wallet Payments*, January 2014.

[6] Funds transfers can be executed using ordinary SEPA instruments: SEPA Credit transfer, SEPA direct debit, SEPA card framework.

different characteristics of the mobile payment services and transaction, for instance consumer to business or consumer to consumer.

The payment system can be analysed under the principles developed by network economics: we are facing a network good when its use depends not only on the preferences and choices by the single consumer, but it is affected also by the behaviour of all the other participants.[7] The consumer's choice depends on direct cost of access to the service (or the purchase cost of a good) and on the costs related to the adoption of the new choice: the so-called switching costs. We have an example of that, when a customer shifts their current account from one bank to another. In the shift from traditional to mobile payment procedures, a switching cost could be the price of a new cellular phone, technologically advanced, but its relevance will be decreasing, alongside the increasing share of smartphones.[8]

When equal access conditions to the payment system exist and switching costs are negligible, consumer's choice will depend only on the fees charged by different providers, so that competition will concern pricing policy. With regard to the speed of execution, new technologies permit a faster procedure than existing ones: different phases of the payment's operation (authentication, account checking, order and confirmation) are shortened, so that distinction between cash and mobile payments could be blurred. This is the case of instant payments, whose execution time is minimal.

In the traditional payment landscape, banks ever had a central position because the use of cards for credit transfer or direct debt requires a final clearing on bank accounts[9]; in the case of e-payments banks maintain their pivotal role, even if consumers use other electronic platforms or internet portals, as in the PayPal scheme, because bank deposit transfers via credit card schemes are required.

A fundamental change could be originated by using mobile network operator (MNO) credit, stored in the mobile device, as means of exchange to make a payment. Functionally, this arrangement is not different from

[7] Fundamental principles of this approach can be found in Oz Shy, *The economics of network industries*, (Cambridge: Cambridge University Press, 2005).

[8] Other switching costs are learning costs and it requires a standardization process of applications to enter a mobile scheme, to minimize costs of changing mobile phone operator.

[9] Payment by e-money, prepaid cards, does not require bank accounts.

when a prepaid card is used, but formally there is not equivalence, due to a different legal regime applied. Only e-money institutions may act as issuers of cards where a monetary value is stored to be spent in general manner, while telephone credit constitutes an advance payment only to be used in a specific way. Further evolution will depend on regulatory schemes and on business strategies conducted by stakeholders like telephone companies.

The evolution of m-payments will probably push to a reallocation of payments services provided by banks and non-bank operators: the focus on access point will be in the future progressively far from usual banking schemes, but banks could rearrange their role from a final access point provider to an intermediate actor, as settlement agent of many others payment service providers. The growth of mobile payments will consist of transactions in traditional stores and, increasingly, of e-commerce operations, easing the participation to the new payment ecosystem of additional categories of operators. This probably will be the more evident feature of the m-payments revolution: the list of all potential stakeholders ready to compete with banking payment services is long, ranging from MNOs to hardware and software manufactures, single or associated, and to e-commerce corporations and internet-related services companies. Each of them can jointly take advantage of scale and scope economies, achieved by gathering different activities in the same business. In this respect banks appear to be less competitive because their activities are not diversified, whereas non-bank operators can provide additional services or other promotional activities to stimulate changes in payment habits.

The banking system will face a crossroads: one strategy will require competition, the alternative one could be an integration with other operators; according to the second option, bank accounts—namely the medium of exchange—would continue to be central in the mobile payments, and traditional banking operations would be replaced by new non-bank procedures. A widespread diffusion of e-commerce will produce change in payment habits and it will not necessarily require new means of exchange, but a different use of the existing ones. Only a massive and growing use of alternative currencies could probably downsize the role of banks.

It is rather difficult, at the present stage of m-payments' evolution, to forecast which tendency will prevail, for two essential reasons: first of all, we do not have—as already stated—a unique scheme acting as reference standard, to guarantee applications' mutual interchange; secondly, the integration process of different stakeholders, mentioned before, is far from being complete, and probably a clear-cut dividing line between payment providers and other correlated services providers will be less meaningful, as mobile payment will become similar to a joint production process. Conditions by which a specific payment innovation could be established derive from a complex balance of competition and cooperation, and for this reason an institutional intervention to push convergence towards a given standard is crucial. However, at present no such agreement exists. In the European case, we had the SEPA experience, where a self-regulatory approach has been realized, in a very different situation, with a lesser number of stakeholders than implied by mobile payments. Even in that case, there have been contrasting outcomes, which raise doubts on an exclusively market-driven solution. Despite shared views on the future evolution[10] by important organizations, it will take a long time before a standard will be established.

European institutions are pursuing the objective of more competition in retail payments, promoting innovative instruments and allowing other operators to enter in a market historically dominated by banks. The recent proposal of a new directive on payment services[11] is coherent with this aim and further contributes to level the playing field between banks and non-banks in the retail payments sector. To make more contestable this market, the new directive allows non-banking operators to access bank accounts for payments execution, diminishing in such a way the traditional competitive advantage constituted by the management of the means of exchange used in remote payment operation. This significant formal innovation will probably reshape the whole payment ecosystem, expanding supply of competitive schemes provided by new entrants. New operators, however, will have a double economic constraint: from one side

[10] As evidence of this joint contribution, see European Payment Council and GSM Association, *Mobile contactless payments service management roles requirements and specifications*, October 2010.

[11] See the revised directive on payment services (PSD2), adopted by European Parliament on October 2015.

the need of recovery high-fixed investment costs to provide new services; but on the other side, they have to adopt a competitive pricing policy to capture former banks' customers. For these reasons, higher competition for banking retail services could come from operators already engaged in the payment system or new operators engaged in other profitable business. The first ones can easily exploit existing resources and scale economies; the others could subsidize initial low-profit activities with revenues of their core business and take advantage of scope economies. When new competitors originate from a different economic sector, they can make attractive a new mobile payment procedure, pairing additional goods or services, or other marketing solutions. In the case of an e-commerce provider, for instance, it could be very difficult to separate the payment service from the sales service, as a further confirmation of the European Commission position,[12] that a distinction between e-payments and mobile payments will increasingly be less evident.

With regard to systemic coherence, there are some doubts that an evolution mainly or exclusively based on a profit maximization approach could be at odds with the assumption that the payment system carries out a public interest function. If payments instruments and procedures enter into a pure market strategy, risks about the stability, soundness and safeness of the payment system could arise.

Issues on Bitcoin

Following the financial crisis, an extended debate has developed on the Bitcoin scheme, a decentralized electronic payments system, proposed in the seminal paper by Nakamoto.[13] In spite of its marginal relevance in global transactions,[14] in a few years the bitcoin's world has attracted an impressive volume of papers, spreading on various fields, and involving not only lawyers and economists, but also mathematicians, politicians,

[12] As clearly stated by European Commission, *Towards an integrated European market for cards, internet and mobile payments*, Green Paper, Brussels, 11 January 2012, p. 5.

[13] Satoshi Nakamoto, *A peer-to-peer electronic cash system*, (2008).

[14] Bitcoin market capitalization on February 2015 was 2.6 billion euro, while M1 aggregate of the Euro area was about 6000 billion euro.

intelligence operators: the reasons for this intense appeal, even by the media, originate from the wide range of expectations that this payment scheme feeds, strictly related to different motivations of its possible use. If compared to the fast diffusion of other payment innovations,[15] the growth of bitcoin's transactions seems low, but, differently from the experience of alternative currencies, it still survives six years after its birth.

There have been many world-wide experiences of non-institutional monies: that is, a situation where people use means of exchange different from legal tender or bank accounts. Usually their circulation is limited to a defined environment, to grant some sort of benefit for firms and inhabitants of a restricted local or regional area, mainly to foster local economic activity,[16] as confirmed by their label of alternative, local or social currencies. They could be considered as vouchers, exchanged at par with legal tender, and used in a general marketing strategy.

Virtual currencies are a completely different case: they are digital entities, neither issued nor regulated or monitored by any public authority like a central bank, or private institution like banks or electronic money institutions (EMI). They are not money in the usual regulated form of legal tender, banking money or electronic money, but they act as accepted money by participants in their specific schemes. Although, since the launch of bitcoin at the beginning of 2009, other similar digital money has been built up, none of them has seen a comparable extension and support by start-up companies and consolidated financial or business operators.[17]

Scholars and authorities have tried to define bitcoin with the goal of clarifying if it should be the object of some type of financial, fiscal or

[15] We think of M-Pesa, for instance.

[16] On this topic see European Central Bank, *Virtual currency schemes*, Frankfurt, October 2012; European Central Bank, *Virtual currency schemes – a further analysis*, Frankfurt, February 2015; Mona Naqvi and James Southgate "Banknotes, local currencies and Central bank objectives", *Bank of England Quarterly Bulletin*, 2013, 4th Quarter; Gerhard Rösl, "Regional currencies in Germany: local competition for Euro?", *Deutsche Bundesbank*, *Discussion paper series 1*: Economic Studies n. 43, (2006); Rolf Schroeder, *The financing of complementary currencies*: *risks and chances on the path toward sustainable regional economics*, The 2nd international conference on complementary currency systems, The Hague, 19–23 June 2013.

[17] Goldman Sachs. "All About Bitcoin", *Top of Mind*, Issue 21, 11 March 2014 is an example.

commercial regulation.[18] We are far away from having reached a shared view. The solutions so far adopted span from a strict ban (China) to recognition as a financial good (Germany) or a commodity (Finland) or an activity requiring specific authorization (USA). Bitcoin has not been recognized as currency, even a virtual one.[19] A recent opinion expressed by the European Central Bank gives a new definition of virtual currency, like bitcoin, as "digital representation of value…which in some circumstances can be used as an alternative to money".[20] Due to the uncertain conversion into legal tender, it denies to bitcoin and similar experiences the status of money.

How the Scheme Works

The Bitcoin scheme does not have a central institution acting as issuer or manager of participants' accounts: it is a peer-to-peer mechanism, where users are at the same time consumers and producers of the medium of exchange. Two private organizations (Bitcoin foundation and Bitcoin.org) are pursuing the objective of fostering the bitcoin experience, especially by information, and software updating, but their role is not essential to the transactions. The issuance of new bitcoins is intertwined with their validation, and it proceeds as Bitcoin's transactions progressively grow. All participants to the scheme have theoretically the same opportunity to enter the validation process, and so to gain new bitcoins. Actually, because the internal algorithm to be solved has an increasing complexity, single users may not normally have available hardware resources needed to do that, and, consequently, the mining function is reserved for a small number of well-equipped participants.

[18] A synthetic analysis has been developed by Reuben Grinberg, "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science & Technology Law Journal*, Vol. 4, December 2011 and by Financial Action Task Force – FATF, *Virtual currencies key definitions and potential AML/CFT risks*, Paris, June 2014.

[19] See for example European Central Bank. *Virtual currency schemes*, Frankfurt, October 2012.

[20] Quoted from European Central Bank, *Virtual currency schemes – a further analysis*, Frankfurt, February 2015, p. 25; the same definition has been expressed in European Banking Authority, *EBA Opinion on virtual currencies*, 4 July 2014.

The lack of a central bank rests on the solution of the trust problem in a transaction mechanism proposed by Nakamoto, according to which the trusted third party (central or commercial bank) is a costly solution, requiring intermediation and transaction costs. We usually accept legal tender or banking money because we trust the state or the banking system, but these institutions simply check that a single unit of money cannot be spent twice at the same time. This multispending problem can be solved by a cryptographic method, which is by a mathematical proof that the payer is the effective owner of that unit of money. A control on the circulation process can be realized by a system of digital signature and a by complex validation process, shared by the same participants: in such a way there is no need of a central bank. Bitcoins are transferred as compensation of a single transaction between two users without account monitoring by third parties: it is the algorithm itself that checks regularity via the process of validation, by which a set of transactions are added to the blockchain. This is a public ledger, freely available to all the participants to the scheme, reporting the sequence of all executed transactions since the beginning of the scheme, in 2009, when the genesis block was created, and the first 50 bitcoins were released and spent by the founder of the system.

Every participant downloads a software application (client software) to be installed on the personal device, where a digital wallet is created, generating an address code to store the bitcoins received.[21] These wallets can be opened at specialized bitcoin service providers or others financial operators accepting bitcoin accounts.[22] Each owner of a wallet can later generate unlimited further address codes to be used for future transactions.

Balances available in each address are used to pay a single transaction, transferring them to the receiving address of the payee. If the outgoing bitcoin payment exceeds the amount to be paid, there will be a reverse transaction for the difference that automatically generates a new address

[21] Bitcoins can be received as payment for business transaction in goods, services or financial instruments, or by charity contribution. Bitcoins are also exchanged with other foreign currencies on specialized electronic platforms. There exist also a very few number of ATMs accepting cash like euros or US dollars in exchange for bitcoins.

[22] Examples are the websites Coinbase.com and Paymium.com: the latter is incorporated under the French law.

code in the sender's wallet. A distinctive characteristic of the Bitcoin scheme is that usually in the wallet the balances do not cumulate in the same address, as in traditional banking current accounts, because each received value would have to be sent to a zero balance address formerly generated.[23] The amount to pay for a new transaction is then managed by the software application, pooling the various addresses in the user's wallet: in such a way a track record of the transferred bitcoins, from one owner to another, is easily done. A transaction does not imply a correspondence between one outgoing address and one destination address, as usual in bank accounts, because balances of multiple outgoing addresses are gathered to the destination address. Every amount of bitcoin can be paired with an identification address, so as to make it possible to verify if the sender is the effective owner.

A digital signature process is the way to prevent multispending: for each single transaction, each participant uses two separate alphanumeric strings, named "keys".[24] Only the public key is transmitted to the network, whereas the private key is needed to couple the owner to the amount transferred[25]; when the payee receives the message from the sender they can easily verify the integrity of the transaction: only if the private and the public keys are correctly paired, the transfer can be done. When the transfer has been executed, it is not yet completed, because the payment has to be validated and this takes about ten minutes: during this time the transaction status is "not confirmed". The transfer of bitcoins is just a message, where much information is included: all used to verify the transaction and to validate it. Each transaction is broadcasted to the nearest nodes and then to the entire network so that all participants, theoretically, can compete to verify it.

Non-confirmed transactions are collected and gathered in a block by nodes that start the validation procedure via a complex cryptographic algorithm: when the node, that is a single participant or a pool of users,

[23] Using a new address for every transaction is a suggested behaviour by bitcoin.org.

[24] When the software generates a new address, the user has an additional pair of private and public keys. The public key represents the code to store or receive bitcoins.

[25] A simplified description can be found in Anton Badev and Matthew Chen, "Bitcoin: Technical background and data analysis", *Federal Reserve Board Finance and Economics discussion series*, 2014-104, October 2014.

finds the mathematical solution, that block is added to other existing blocks in the blockchain. The blockchain is the sequence of all transactions executed from the beginning and its structure prevents that a payment could be cancelled once it has been submitted to the network.[26] The transaction included for the first time in the block receives a confirmation; later when other blocks of additional transactions are verified and added to the blockchain, the original transaction receives a second confirmation message and so on, until the sixth confirmation. This last confirmation states that the original transaction is included (and verified) in six blocks: at this point the transaction's status will change to "confirmed" and the amount of bitcoin transferred will be effective; the payment from the sender to the payee is then completed. New blocks are of variable length: they are composed of a different number of transactions and different values of bitcoins transferred.[27]

The validation process plays a central role in the scheme, since it allows a function usually carried out by central banks in traditional payment systems: in the Bitcoin scheme this function is decentralized via a peer-to-peer mechanism[28]; this is an example of cooperation (all nodes contribute to validate blocks) in a competitive form, because the first node which solved the algorithm to validate a block is rewarded by new bitcoins, generated by the system itself. This second aspect is crucial in the supply of bitcoins. Validation is at the same time a means to permit bitcoins to be accepted as a medium of exchange and the issuance mechanism, not directly controlled by third parties. The reward halves every four years, corresponding to 210,000 new blocks added to the blockchain,[29] as determined by an internal growth rule: this activity is conducted on a voluntary base and its participants are named "miners", just like the gold mining in the past. We already stated that solving the mathematical problem to validate a new block is progressively more difficult, thus

[26] The complex algorithm used in the scheme makes impossible a recalculation of the whole sequence, so a transaction cannot be denied by the sender.

[27] Useful information on daily transactions are reported in the website blockchain.info where in real time one can see progression of the new blocks verified and added to the blockchain.

[28] This democratic feature is more apparent than real, due to growing difficulty of validation proof and to the consequent requirements of expensive processing machines and energy.

[29] Every day about 144 new blocks are added to the blockchain.

making the validation process unsuitable for single participants lacking ample resources: the resulting concentration in mining also leads towards pool-mining, accessed by single users to share the generated revenues.

Besides the new bitcoins granted to miners of new blocks, a voluntary fee on every submitted transaction constitutes a further form of compensation: when the validation process is completed the user pays a variable amount[30]; even if this fee is completely on a voluntary basis, probably transactions without fees are never validated.

To foster the bitcoin process of payment many operators have entered the "bitcoin's ecosystem" and they act as service providers to make transactions easier: in a strict sense, their function is not essential to the mechanism described above, but it surely has had a positive impact on bitcoin's acceptance by users and merchants. These services concern three categories: transaction facilities, real-time exchange with other currencies, information and communication; all are provided by web-based firms. "A growing number of start-ups has been emerging to provide new virtual currency products and services that facilitate use of decentralized virtual currency payments network, particularly bitcoin."[31] These firms are wallet providers, virtual currency payment processors, virtual currency exchangers and bitcoin automated teller machine (ATM) operators[32]; this is an example of how an infrastructure can autonomously grow, even if its existence had not been considered at the launch of the system. Wallet providers facilitate users in managing bitcoins and exchangers guarantee convertibility with fiat currencies, minimizing in such a way the time spent to transact. The most important function is probably that of payment processors, particularly for merchants. When a merchant receives a bitcoin balance they can immediately convert it into traditional money, so as to prevent intraday volatility and possible losses. A fundamental complementary service is to reduce volatility and improve connection

[30] Usually 1 % of the value transferred is charged on sender: variable fees can be applied according to the type of transaction, as explained in the website bitcoin.org. Transactions can be labelled as high-priority, depending on fee and on creation date of bitcoins used, to stimulate spending of idle amounts stored in wallet.

[31] Quoted from Financial Action Task Force – FATF, *Guidance for a risk-based approach to virtual currencies*, Paris, June 2015, p. 43.

[32] There are only a few manufacturers of bitcoin ATM: at the end of 2014 there were about 300 machines operating in the world, provided by merchants accepting bitcoin payments in their shop.

with the traditional payment systems, making available bitcoin facilities on financial accounts with SEPA address codes. In such a way traditional or new payment service providers could act as risk-taking operators, managing daily volatility.

The growing infrastructure firms engaged in mining activities concentrate computer capacity in an industrial plant, using specific high-power machines manufactured by specialized hardware vendors; in such a form, mining activity is not anymore a single user's participation to the feasibility of the scheme and it becomes an effective business activity.[33]

Why Use Bitcoins?

There are different reasons why people use bitcoins: the first one rests on ideological behaviour and is a rather weak motivation to investigate the future perspectives of the scheme. Libertarian users prefer a medium of exchange not fostered by the state, and, in particular, a payment system where banks or other financial intermediaries are not engaged at all; this position, certainly a minority, can be considered as a consequence of a general criticism, following the crisis of 2008, towards banking and finance operators as representatives of a disruptive financial world, in conflict with a sound real economy.

One can devote more relevance to the second category of motivation: the illegal one. Illegal activities such as money laundering, trading weapons and drugs, or terrorism financing are globally widespread and certainly could take advantage from a peer-to-peer procedure such as the Bitcoin scheme that allows a high degree of anonymity. Another Bitcoin activity, even if not considered illegal, is online gambling. According to a recent estimate by the Federal Reserve in mid-2014[34] almost a half of all transactions in bitcoins could originate from that.[35]

---

[33] At the end of 2014 the whole of daily gross revenues from mining activity has been estimated about 1 million US dollars.

[34] See Anton Badev and Matthew Chen, "Bitcoin: Technical background and data analysis", *Federal Reserve Board Finance and Economics discussion series*, 2014-104, October 2014.

[35] According to Anton Badev and Matthew Chen, "Bitcoin: Technical background and data analysis", *Federal Reserve Board Finance and Economics discussion series*, 2014-104, October 2014, p. 19,

The third category of motivations invoked in using bitcoins refers to individual economic convenience. This has to be distinctly considered from demand and offer sides: individual users of the new payment scheme (consumers and merchants) are pushed by a reduction in costs and time requested in transferring money, easy access to the payment system and the global reachability; firms offering bitcoin correlated services—or virtual currencies payment products and services, according to Financial Action Task Force's (FATF) definition—are more interested in easier way to make business, selling everything related to the innovative process. Furthermore, as stated in the introduction, many other sectors consider as the true innovation of Bitcoin its record system, that is the cryptographic method to build the public ledger. The joint use with a mobile device fosters Bitcoin's diffusion among non-banked or underbanked people that frequently transfer small amounts of money, even across countries: in this sense the Bitcoin scheme can help financial inclusion. The lack of regulation, the absence of third parties and of exchange rate fees lessen the total cost of the payment; foreign remittances are usually charged for a fee of 5 % on average, when money transfer operators' services are used, while the average voluntary fee applied in the bitcoin scheme is about 1 %.[36]

Traditional banking operators have tried to compete on this aspect, offering easier access to payment instruments, like various solutions of home and phone banking. Furthermore, further competitive pressure could come from the expected rapid growth in instant payments, also coming from non-bank payment service providers with a bitcoin system.

Users exhibit their preferences on the conviction that all different instruments are equally safe and unaffected by security, privacy or fraud problems; when alternative payments instruments and procedures are provided by non-bank operators coming from different business activities, one can wonder if all these aspects are fulfilled in a convenient manner, in the way that banks usually do.[37]

---

a large volume of small value bitcoin transactions originate from the online gambling service Satoshi Dice.

[36] Remittances are globally growing, so this will be an attractive business in the future.

[37] On this topic see European Central Bank, *Recommendations for the security of mobile payments*, Frankfurt, November 2013.

So far we have considered only benefits in using bitcoin, without discussing the potential risks users will be exposed to. A report published by the European Banking Authority in 2014[38] listed all the possible risks affecting individual positions and systemic aspects: individual risks refer to users, merchants and other market participants; systemic risks can arise from default of payment system providers, due to interdependencies between schemes where fiat currencies are used and virtual currency schemes.[39] A general condition regards correct information about risk: this function is provided only in an informal way by different agents and that prevents users from understanding all the features of the schemes. As a "digital representation of value", bitcoins are obviously exposed to operational risk; due to hardware malfunction or software collapse, bitcoins stored in a personal wallet or in external accounts may vanish completely. In case of fraud there is no form of legal protection or jurisdiction that a user can invoke, so it is impossible for any form of reimbursement. For the same reason, in absence of regulation, fraudulent events or closing activity of exchange platforms or wallet providers can cancel customers' bitcoin balances. Furthermore, since bitcoins are considered "private money", that is voluntarily accepted, there is not an absolute guarantee that one can use the amount received with other people; so the bitcoin cannot be a widely accepted medium of exchange. Even in respect of another traditional monetary function, that of store of value, the bitcoin seems inadequate, due to the high volatility of its exchange rate with other fiat currencies. Holding bitcoin as a possible use of personal financial wealth is hazardous, since the user is exposed to high capital losses.[40]

[38] See European Banking Authority, *EBA Opinion on virtual currencies*, 4 July 2014.

[39] See European Banking Authority, *EBA Opinion on virtual currencies*, 4 July, 2014, p. 35. Issues in the following text are reported from a Bank of Italy warning. See Banca d'Italia "Avvertenza sull'utilizzo delle cosiddette valute virtuali", Rome, 30 January 2015.

[40] The main reason is the high volatility on bitcoin exchange rate: its value in terms of US Dollar was about USD 0.001 at the launch of the scheme on 2009; USD 0.10 on October 2010. On December 2013, 1 bitcoin was exchanged with over USD 1,200.

Perspectives and Criticism

The Bitcoin scheme has been considered a powerful driver of innovation[41] with many stakeholders, ranging from hardware manufacturers to payment service providers: operators from the offer side are showing growing interest in building new payment procedures and alternative systems of decentralized recording[42] to be applied in other business sectors. Furthermore, it is not surprising that a lot of financial institutions regard Bitcoin, or its internal architecture, as a way to escape stringent regulation and to lessen transaction costs: for them, virtual currencies could became an additional opportunity to make profits, and such a behaviour normally stems from finance industry, and public authorities seem to stimulate tendencies in the same vein.[43] The purpose to establish national global players in finance requires sometimes a loose behaviour towards unregulated innovative processes.

As the SEPA project reveals, competition in retail payment is fruitful, and it involves governance aspects, since a self-regulation approach is clearly different from a "do-it-yourself" money; nevertheless, the possibility to build an unregulated tailored payment system for specific needs seems now widely accepted.[44] For these reasons, enthusiastic opinions on Bitcoin (and on its expected evolution) could be interpreted as a grow-

[41] European Banking Authority, *EBA Opinion on virtual currencies*, 4 July 2014, recognizes that in the European case benefits will probably be less than risks; central banks consider it an innovation, with potential risks depending on its use by consumers, as stated in European Central Bank. *Virtual currency schemes – a further analysis*, Frankfurt, February 2015.

[42] For suggestions in this sense see The Economist. "Blockchains: The great chain of being sure about things", 31 October 2015.

[43] For example a British Government's document states this intention to "... set out plans for making Britain the global centre of financial innovation..." announcing "....pro-innovation regulatory measures to unlock the potential of new technology, and allow new innovators to compete on a more level footing with established players" enabling "... the government to examine the potential benefits that digital currencies could bring to consumers, businesses and the wider economy". Quoted from H.M. Treasury. *Digital currencies*: *call for information*, 18 March 2015, para. 1.

[44] François Velde, "Bitcoin: a primer", *Chicago FED letters*, Federal Reserve Bank of Chicago, December 2013, p. 4, suggests that financial institutions "...could issue their own bitcoins, using bitcoin technology as public ledger and cryptography".

ing belief that a programmable money[45] will be soon feasible: it would act as a medium of exchange, or commodity, or base element for structured financial products, but it will not be money in the conventional sense in the prevailing past.[46] Past and current experiences show that a private money could normally exist, in a closed loop of users, when it is voluntarily accepted. The question concerns potential externalities produced, since competition on payment instruments is not competition on means of exchange: the evolution from a situation of central bank's legal monopoly, to a completely different one, where money could be part of a commercial value chain, can originate risks at micro and macro level.

A first criticism regards the convenience to promote the use of a certain means of exchange as part of commercial strategies: alternative payment instruments and procedures, when the critical balance between competition and cooperation holds, foster efficiency, if consumer's security is not reduced; jointly, merchants and payment service providers could adopt inadequate and unsound behaviours,[47] so that consumers might not correctly perceive hidden risks related to unregulated peer-to-peer payment schemes. The correct operation of the payment system has always been considered a public interest function, not a profit maximizing activity.

The second criticism stems exactly from here: a private money scheme could have a negative impact on the payments' ecosystem, when firewalls do not exist and many matters remain unresolved, due to the unclear functional, institutional and legal definition of virtual currencies. On the one side monetary and regulatory authorities attempt to limit bitcoins' use and to prevent contagion risks; on the other side, there is a global finance industry that actively works to increase bitcoins' transactions, providing real-time conversion and other services. Systemic effects could arise from

[45] This definition has been used by Pak Nian, Lam and David Lee Kuo Chuen. "Introduction to Bitcoin", in David Lee Kuo Chuen, (editor). *Handbook of digital currencies*. (Amsterdam: Academic Press, 2015)

[46] According to George Selgin, Synthetic commodity money, 10 April 2013. Available at SSRN: http://ssrn.com/abstract=2000118, there are four different monies: bitcoin is a synthetic commodity money. Other analysis can be found in David Yermack, "Is Bitcoin a real currency? An economic appraisal", in David Lee Kuo Chuen (editor). *Handbook of digital currencies*. (Amsterdam: Academic Press, 2015) and in Stephanie Lo and Christina Wang. "Bitcoin as money?", *Current perspectives*, Federal Reserve Bank of Boston, n. 14-4, September 2014.

[47] Security and privacy considerations are crucial in this sense. See in this book the contribution of Safari Kasiyanto.

overlapping[48] positions of financial operators simultaneously engaged in bitcoin and other currencies. In case of failure of an exchange site, for instance, the following lack of confidence could extend beyond the Bitcoin scheme, damaging confidence also on traditional payment systems. Let us suppose that suddenly all bitcoin wallets of an electronic platform vanish, due to a hacker attack or a technological default[49]: losses of financial operators could originate a contagion effect; since the scheme does not have an issuing central board, unexpected needs of additional bitcoins to provide confidence would not be fulfilled at all. The Bitcoin algorithm supplies the means of exchange at a pre-defined rate and it prevents creating—that is, spending—non-existing bitcoins. This mechanism does not require a central bank, or even a private supervisory body, to keep confidence rested on public ledger solutions to multispending problems, but this is not the case when a rescue operation has to be done: and so one has to wonder if really a lender of last resort is unnecessary, when cryptocurrencies are used.

About 20 years ago, when first experiences of e-money were launched[50] many scholars raised similar arguments about the central banks' role; more recently, fears about stability of payment system has been renewed when discussing payment institutions' activity, regulated by the European payments services directive. In both cases, the expected negative effects have not been fulfilled, and one may think the same will happen with regard to bitcoins. These situations were rather different from the existing one, since the e-money diffusion required specific devices to be used by consumers, whereas development of payment institutions needed a deep involvement by other non-banking operators like MNOs or large retailers.[51]

In the case of a "digital representation of value", like bitcoin, the key development factor of new payment procedures rests mainly on people's

[48] In Financial Action Task Force – FATF. *Guidance for a risk-based approach to virtual currencies*, Paris, June 2015, p. 4 attention is concentrated on exchangers, where "convertible virtual currencies activities intersect with regulated fiat currency financial system". Same issues are expressed in European Banking Authority, *EBA Opinion on virtual currencies*, 4 July 2014 and in European Central Bank, *Virtual currency schemes – a further analysis*, Frankfurt, February 2015.

[49] An example was the Japanese Mt. Gox platform, closed down on February 2014.

[50] Considering e-money as a "prepaid valued fixed on hardware device" according to ECB definition.

[51] A further aspect is that many key actors of the virtual currencies environment were not present before: many of them are start-up firms, their managers are strongly motivated and their marketing strategies are highly dynamic

payment behaviours, as we have argued analysing the switching costs' problem: if these will be falling to zero, a further strong impulse to innovate could arise. Bitcoin will probably continue to exist as a means of exchange, but its extension scale will crucially depend on future improvements, currently hard to envisage. However, one can see a contradiction in the current tendencies so far exhibited, due to inadequacy of the original environment, based on a peer-to-peer voluntary participation, whose incentives are progressively diminishing, so the "libertarian" vision of a free and global means of exchange, fully separated by finance and banking institutions will probably evolve in, a more realistic view, a private business.

The original voluntary approach could be inadequate, and a transformation into a profit seeking environment will probably occur, as big financial companies' attention suggests. A set of more structured monitoring and coordination bodies, like the existing Bitcoin foundation, will have to be realized, to improve a support function, making available complete and standardized information to potential users.

From an economic viewpoint, however, when mining's revenues will get close to zero, the current fees of about 1 % could increase, hindering the expansion of the scheme. A way to escape from this difficulty requires economies of scope, that is, stable connections with financial intermediaries: pursuing a wide range of business activities, they could foster a pricing policy to maintain existing very low transaction fees charged. One cannot obviously neglect that a tendency towards high concentration would be in clear contradiction with the decentralized principle.

The current tendencies in bitcoin mining support this view: if we look at the entities adding new blocks at the blockchain we recognize that the first four (F2pool, Antpool, Bitfury, Btcc pool) account for nearly three-quarters of transactions.[52] These companies acting as big miners are manufacturers of bitcoin-dedicated hardware: they are not third parties in the usual sense of payment systems, but their action, seemingly separated from service providers, is fundamental to maintain and develop the scheme. Their activity could be envisaged like an oligopolistic issuing function, making the Bitcoin scheme of payment more similar, from this viewpoint, to the existing ones.

[52] As reported from Blockchain.info in 1 November 2015.

References

Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014a). Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin, 54*(3), 262–275.

Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014b). The economics of digital currencies. *Bank of England Quarterly Bulletin, 54*(3), 276–286.

Au, Y., & Kauffman, R. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Application, 7*(2), 141–164.

Badev, A., & Chen, M. (2014, October). Bitcoin: Technical background and data analysis. *Federal Reserve Board Finance and Economics Discussion Series*, 2014-104.

Banca d'Italia. (2015, January 30). *Avvertenza sull'utilizzo delle cosiddette valute virtuali*. Rome: Banca d'Italia.

Board of Governors of the Federal Reserve System. (2015). March). *Consumers and mobile financial services 2015*. Washington, DC: Board of Governors of the Federal Reserve System.

Committee on Payment and Settlement Systems (2012, May). *Innovations in retail payments*. Basle: Bank for International Settlements.

Committee on Payments and Market Infrastructures (2014, September). *Non-banks in retail payments*. Basle: Bank for International Settlements.

Dennehy, D., & Sammon, D. (2015). Trends in mobile payments research: A literature review. *Journal of Innovation Management, 3*(1), 49–61.

European Banking Authority – EBA (2014, July 4). *EBA opinion on virtual currencies*. London: EBA.

European Banking Authority – EBA. (2013, December 13). *Warning to consumers on virtual currencies.* London: EBA.

European Central Bank. (2009, December). *Retail payments – Integration and innovation*. Frankfurt: European Central Bank.

European Central Bank. (2011, October). *The future of retail payments*: *Opportunities and challenges.* Frankfurt: European Central Bank.

European Central Bank. (2012, October). *Virtual currency schemes*. Frankfurt: European Central Bank.

European Central Bank. (2013, November). *Recommendations for the security of mobile payments*. Frankfurt: European Central Bank.

European Central Bank. (2014, June). *Retail payments at a crossroads*: *Economies*, *strategies and future policies*. Frankfurt: European Central Bank.

European Central Bank. (2015, February). *Virtual currency schemes – A further analysis*. Frankfurt: European Central Bank.

European Commission. (2012, January 11). *Towards an integrated European market for cards, internet and mobile payments*. Green Paper, Brussels.

European Commission. (2013). *Proposal for a directive of The European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC*, COM/2013/0547 final.

European Payment Council. (2014a, January). *White Paper mobile wallet payments*. Brussels: European Payments Council.

European Payments Council. (2014b, December). *Overview on mobile payments initiatives*. Brussels: European Payments Council.

European Payments Council and GSM Association. (2010, October). *Mobile contactless payments service management roles requirements and specifications*. Brussels: European Payments Council.

Financial Action Task Force – FATF. (2014, June). *Virtual currencies key definitions and potential AML/CFT risks*, Paris: FATF.

Financial Action Task Force – FATF. (2013, June). *Guidance to a risk-based approach to prepaid cards, mobile payments and Internet-based payments services*, Paris: FATF.

Financial Action Task Force – FATF. (2015, June). *Guidance for a risk-based approach virtual currencies*, Paris: FATF.

Financial Crimes Enforcement Network – FinCEN. (2013, March 18). *Application of FinCEN's regulations to persons administering exchanging or using virtual currencies*. FIN 2013-001. https://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

Financial Crimes Enforcement Network – FinCEN. (2014, October 27). *Request for administrative ruling on the application of FinCEN's regulation to a virtual currency payment system*. https://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf.

Goldman Sachs, (2014, March 11). All about Bitcoin. *Top of Mind*, *21*, 3–21.

Grinberg, R. (2011, December). Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal, 4*, 159–208.

Jack, W., & Suri, T. (2011, January). *Mobile money: The economics of M-Pesa*. NBER Working Paper, n. 16721.

Lee Kuo Chuen, D. (Ed.) (2015). *Handbook of digital currencies*. Amsterdam: Academic Press.

Lo, S., & Wang, C. (2014, September). Bitcoin as money? *Current perspectives*. Federal Reserve Bank of Boston, n. 14-4.

Nakamoto, S. (2008). Bitcoin: *A peer-to-peer electronic cash system*. Available at: https://bitcoin.org/bitcoin.pdf.

Naqvi, M., & Southgate, J. (2013). Banknotes, local currencies and Central bank objectives. *Bank of England Quarterly Bulletin, 53*(4), 317–325.

Pak, N. L., & Chuen, D. L. K. (2015). Introduction to Bitcoin. In: D. Lee Kuo Chuen (Ed.), *Handbook of digital currencies* (pp. 6–30). Amsterdam: Academic Press.

Rösl, G. (2006). Regional currencies in Germany: Local competition for Euro? *Deutsche Bundesbank*, *Discussion paper series 1*: Economic Studies n. 43.

Schroeder, R. (2013). The financing of complementary currencies: Risks and chances on the path toward sustainable regional economics. *The 2nd International Conference on Complementary Currency Systems*, The Hague, 19–23 June 2013.

Selgin, G. (2013, April 10). *Synthetic commodity money*. Available at SSRN: http://ssrn.com/abstract=2000118

Shy, O. (2005). *The economics of network industries*. Cambridge: Cambridge University Press.

The Economist. (2015, October 31). *Blockchains: The great chain of being sure about things*. London: The economist newspaper.

Treasury. (2015). *Digital currencies*: *Call for information*. Available at: https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information.

United States General Accountability Office – GAO. (2014, May) *Virtual currencies*. Washington DC: United States General Accountability Office.

Velde, F. (2013, December). Bitcoin: A primer. *Chicago FED letter.* Federal Reserve Bank of Chicago, Chicago.

Yermack, D. (2013, December). *Is Bitcoin a real currency?* NBER Working Paper Series, n. 19747.

Yermack, D. (2015). Is Bitcoin a real currency? An economic appraisal. In D. L. K. Chuen (Ed.), *Handbook of digital currencies* (pp. 31–44). Amsterdam: Academic Press.

Part II

The Framework: A European and Comparative Outline

3

Bit by Bit: Assessing the Legal Nature of Virtual Currencies

Noah Vardi

Abstract "Virtual currencies" are a monetary phenomenon not easily defined. They set themselves at the crossroads between money, investment instruments, possibly commodities, and notwithstanding the fact that they are relatively widespread in practice (Bitcoin is the most prominent example), they are still lacking specific regulation in almost all legal systems. This poses a series of problems and risks that have caught the attention of regulators and market operators, some of whom have recently released important studies highlighting the need for ad hoc rules. The paper aims at giving a brief overview of the legal nature of these currencies and the possible rules which may be applied to them pending the approval of specific legislation.

N. Vardi (✉)
Associate Professor, University of Roma Tre, Law School, Italy

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_3

Introduction

The "paradox" of virtual currencies is that in trying to define them from a normative point of view, it is easier to conclude what they are not, rather than what they are. A paradox all the more evident, when considering that a "currency" quintessentially requires a statutory definition. Virtual currencies, on the contrary, lack both a normative definition and broader still, any form of legal regulation. The "synthesis" of this syllogism that can be easily deduced is that virtual currencies are not, strictly speaking, "currencies".

The legal vacuum surrounding virtual currencies renders them both extremely attractive and dangerous: neither illegal (mostly), nor prohibited, but still outside the domain of the law. The absence of regulation, however, does not mean that the phenomenon as such is not under close scrutiny of several agencies, governmental authorities, market operators and institutional actors.[1]

The question that thus arises is whether and how markets, users, and regulators can cope with this legal vacuum. As a partial anticipation of the conclusions that some of the following considerations will lead to, a distinction should be made. A legal vacuum may not be so dangerous, as long as one stays within the domain of private autonomy, where certain existing tools may come to aid. When considering systemic risk, on the other hand, it seems that positive intervention may be required.[2]

[1] There is a wide number of studies and reports, commissioned especially by national and transnational Banking Authorities that have examined the phenomenon of 'Virtual Currencies'. In some cases these studies also contain tentative assessments of the risks associated with the use of virtual currencies, and/or a series of related 'warnings' to the public. References to these documents will be made throughout the text, however some of the most thorough, *inter alia*, can be recalled: European Central Bank, *Virtual Currency Schemes*, October 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, accessed July 2015; European Banking Authority (EBA), *Opinion on* '*virtual currencies*', July 2014, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-201408+Opinion+on+Virtual+Currencies.pdf, accessed July 2015; Law Library of Congress, *Regulation of Bitcoin in Selected Jurisdictions*, http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf, accessed July 2015; Financial Action Task Force, *Virtual Currencies. Key Definitions and Potential AML/CFT Risks*, June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, accessed September 2015.

[2] The EBA opinion on virtual currencies for example has singled out more than 70 risks across several categories, including risks to users; risks to non-user market participants; risks to financial integrity; risks to existing payment systems in conventional fiat currencies; risks to regulatory authorities (See EBA *Opinion on* '*virtual currencies*', 5).

Before trying to assess virtual currencies from a legal point of view a few brief words on how they work should be spent. The mechanism is quite complex and alien to non-specialists and the technicalities are beyond the scope of this paper. There are currently different schemes of so-called "virtual currencies" and each of them poses different problems.

More specifically, virtual currencies have been classified according to their relation with "real money" and the "real economy", that is, by taking into account if and how the monetary flow between virtual currencies and real currencies work, and if and how virtual currencies can be used to purchase real goods and services. According to these parameters, the existing virtual currency schemes have been divided into (i) closed virtual currency schemes (that have scarce, if any, interaction with the real economy, and include currencies used for online games); (ii) virtual currency schemes with unidirectional flow (that imply an irreversible conversion at a specific exchange rate from the "real currency" to the "virtual currency" that can then be used both to buy virtual and real goods and services, and include "credits", "vouchers", "points" or other "bonus" systems); (iii) virtual currency schemes with bidirectional flow (virtual currencies can be bought and sold according to exchange rates with real currencies and can be used to purchase both virtual and real goods and services; they include Bitcoins).[3]

However, the type that is under closest observation (and that also enjoys one of the widest circulations at the moment) is the Bitcoin, one of a series of so-called "peer-to-peer" electronic cash systems.[4] The Bitcoin scheme can serve as a useful paradigm not only of the way in which virtual currencies work, but also of the reasons for their success and the concerns they raise.

Bitcoins are considered as "cryptocurrencies" specifically because they rely on a mechanism of peer-to-peer cryptography for the validation of transfers. Users can exchange Bitcoins (electronic tokens) through a mechanism of verification known as "mining" which is based on a

[3] For this classification, see ECB, *Virtual Currency Schemes*, October (2012): 13–15

[4] A first-hand illustration of the Bitcoin can be found in the document authored by their (presumed) inventor, who goes under the pseudonym of Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, accessed September 2015.

public ledger that records "ownership" of the digital currency. When the owner of a Bitcoin transfers it to a recipient, a group of so-called "miners" consults the ledger to verify the owner's claim of ownership, solves a complex cryptographic problem, and annotates the transfer to the recipient by logging the transaction on the ledger (where the recipient will now appear as the new owner). As a "reward" (and as an incentive) for the activity of mining, which involves the solution of complex sequences of algorithms, the "miner" that solves the cryptographic problem is awarded with a new batch of cryptocurrencies that are automatically generated by the software.

Given that the number of possible combinations of algorithms is finite and as long as the creation of new Bitcoins through mining activity keeps a geometric rate of growth, it is possible to estimate both the maximum number of Bitcoins (about 21 million) that can be potentially "minted" (or "mined") and the moment in which this plafond will be reached (in 2140). This renders Bitcoins chattels that are, to a certain extent, potentially "scarce", given their finite number; and it is precisely due to this characteristic, that some observers have expressed some fears regarding a possibly inherently "deflationary" nature of these tokens.[5]

A fundamental feature of this mechanism is that it is decentralized and "private", since the public ledger that records ownership of the Bitcoins functions without the control or the need either of a central bank, or of a private bank or other credit institution and without a central clearing house. This decentralized system does not confer a power of control on monetary emission or of liquidity to a single central institution and according to the ideology behind Bitcoin, this avoids some of the "effects" (namely, inflation) of central banking policies. It comes as no surprise thus, that some observers have recalled analogies between the ideology of the Bitcoin and the doctrines of the Austrian School

[5] A sudden raise in their price of 'purchase'/demand, provoked by an increase in the number of users, might incentivise users not to spend the Bitcoins but rather keep them as 'scarce chattels' See ECB, *Virtual Currency Schemes*, cit., at p. 25, (with some criticisms towards these theories); See also Reuben Grindberg, "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science & Technology Law Journal* 4 (2012): 177 ff.

of Economics and that some commentators have referred to Bitcoin as "Hayek money".[6]

Virtual Currencies and Money

After this brief overview on the concrete functioning of the Bitcoin, taken as a paradigm of virtual currencies, it is now possible to attempt an assessment on the legal nature of these "tokens". The first consideration that comes to mind is that the epithets of "cryptocurrencies" or "virtual currencies" are misleading. Indeed, in order for a money to be qualified as a "currency" it must have the status of legal tender, conferred by the national monetary laws. At the moment, there is no national law that recognizes this status to Bitcoins.[7]

Furthermore, the mechanism itself with which Bitcoins are "minted", that is through peer-to-peer "mining", without any intervention on behalf of a central bank or national minting authority, confirms that there is almost a contradiction in terms between the ideology underlying Bitcoins and the idea of a national legal tender. The absence of this quality confirms that Bitcoins cannot be considered as an official currency.

A first consequence regarding the identification of a possible legal nature of Bitcoins and the applicability of rules ensuing from this qualification can, however, be made already at this point: the exclusion of the status of "currency" as legal tender to Bitcoins entails that all regulation regarding payments in legal tender, in which tender qualifies, for example, the exact performance and the discharge of the debtor, cannot be applied

---

[6] See Ferdinando M. Ametrano, *Hayek Money*: *the Cryptocurrency Price Stability Solution*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270), highlighting that Bitcoins could be considered as the practical implementation of the theories of the Austrian School of Economics, especially those on the 'denationalisation of money' illustrated by Friedrich A. von Hayek in his book *The Denationalisation of Money* published in 1976.

This analogy, however, has also been met by criticism by some scholars who have highlighted that Bitcoins have no intrinsic value comparable to the gold standard nor do they meet the requirement of the 'Misean Regression Theorem' according to which acceptance and circulation of money depends on an intrinsic value it possesses (due to the fact that it is rooted in a commodity with purchasing power). See ECB, *Virtual Currency Schemes*, 23.

[7] See i.e. the overview in the Study of the Law Library of Congress, *Regulation of Bitcoin in Selected Jurisdictions*.

to these "cryptocurrencies". This concerns, for example, the rules on the nominalistic principle (often considered as the legal transposition of the notion and principle of a legal tender); it also applies to rules excluding or allowing monetary clauses where the reference is to a fiat currency or to an index measuring an exchange rate between fiat currencies.

These considerations do not exclude, however, that the nature of "money" of these coins may be further questioned. Money and currency are indeed two separate notions and the first may exist without the second, especially if one considers "complementary" currencies. The next logical step is thus to examine if and to what extent these virtual currencies qualify as "money".

The legal nature of money is traditionally identified with three functions: (i) money as a means of exchange; (ii) money as a unit of account; (iii) money as a store of value. Bitcoins (and other virtual currencies belonging to the other two schemes identified above) are used for the exchange between a "unit of account" and (virtual or real) goods and services. The first and second functions normally attributed to money are thus—potentially—identifiable in these tokens.[8] What is more surprising, furthermore, is that the third and last function, that of a store of value, can also to some extent, be found in Bitcoins, and this last feature has raised major concerns, especially by market supervision authorities since the function of "store of value" may be dangerously close to that of an investment "instrument" (and the latter are closely supervised and regulated in many legal systems).[9]

---

[8] Some observers have, however, highlighted that these functions are not really fully carried out by Bitcoins due to a series of practical reasons, including, *inter alia*, their limited circulation in practice in retail transactions for the purchase of goods and services, and the complexity in actually measuring prices in Bitcoin. See David Yermack, "Is Bitcoin a Real Currency? An economic appraisal", NBER Working Paper No. 19,747, December 2013 9–11.

[9] In a recent, rather known case decided in the United States, (*SEC* v. *Shavers*, US District Court, Eastern District of Texas, (2013), 2013 US Dist. LEXIS 110018), concerning a Ponzi scheme carried out using Bitcoins, the Court stated, *inter alia*, that Bitcoins are a form of currency; the Securities Act of 1933 defines a 'security' as 'any… investment contract' and the Court, applying the so-called 'Howey test' set down by the Supreme Court in *SEC v. W.J. Howey Co.*, (328 US 293, (1946)), held that Bitcoins can be qualified as investment contracts (that is, according to the test, 'any contract, transaction, or scheme involving (1) an investment of money, (2) in a common enterprise, (3) with the expectation that profits will be derived from the efforts of the promoter or athird party'); thus Bitcoins constitute an investment of money for the scope of the Securities Act.

The function of "store of value" could be attributed to Bitcoins, specifically, if one takes into consideration the possible analogy between the finite number of coins that can be "mined" and put into circulation, and the mechanism of the gold standard which historically has characterised more than one national currency.[10] However, the very high volatility rate of the Bitcoin registered thus far may undermine its use as a store of value.[11]

Virtual Currencies and Electronic Money

The possibility of assessing Bitcoins as a form of "money" (though not currency) does not imply that the regulation on electronic money is applicable straightforwardly to these tokens. On the contrary, and notwithstanding the "digital" nature of Bitcoins, the European rules on e-money, for example, cannot be applied to Bitcoins given that they lack two requirements set forth by the Electronic Money Directive.[12] Namely, e-money can be issued only in exchange for the transfer of corresponding funds in real currency at par value (article 2, n. 2, and article 11, Directive 110/2009/EC), and e-money must be redeemable into real currency at any moment and at par value upon request of the electronic money holder (article 11 Directive 110/2009).

The consequence in terms of regulation that follows from this exclusion is that the prudential and supervisory regulation which applies to the emission of e-money cannot be applied to the activity of emission of virtual currencies (including Bitcoins).

[10] The idea of a limited quantity of coins (though not yet reached) may have, *inter alia*, been at the basis of two 'Bitcoin rushes' that took place in 2011 and in 2013. This mechanism has been severely criticised by many, including, for example, the economist Paul Krugman, *inter alios*, in a few op-eds published by the *New York Times* that have been quoted extensively: "Golden Cyberfetters" published on 7 September 2011, followed by "BitCoin is Evil", published on 28 December 2013.

[11] See David Yermack, "Is Bitcoin a Real Currency? An economic appraisal", 15, who takes into account the data on Bitcoin exchange rates with major fiat currencies as of 2013.

[12] Directive 2009/110/EC of 16.9.2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, in *OJ* L267, of 10 October 2009, at p. 7.

Virtual Currencies and Complementary Currencies

The difficult classification of Bitcoins within a legal category of money (with the consequent unfeasibility of extending by analogy most of the existing regulations on money to Bitcoins), confers, according to some observers, a great competitive advantage to these tokens, which can be used more or less freely and without any supervisory or prudential constraint that applies to other forms of "money".

This would make Bitcoins particularly attractive on the one side for the use for online transactions (thus competing with other "systems of payment" used for e-commerce) given its very low transaction costs, its use for micropayments, its anonymity (the sequence of transactions to and from Bitcoin accounts are visible to the public, but there is no link between the accounts and individuals)[13]; on the other, for the use as a "store of value" in competition with other "real" currencies, especially those anchored to the gold standard.[14]

Given their characteristics, an analogy can more easily be found between Bitcoins and so-called "complementary" or "alternative" currencies. The latter are mostly regulated exclusively by private autonomy. Their circulation depends only on a consensual basis (and on the trust of the parties) and it is (or may be) recognized by legal systems as a choice on the "means of payment" falling within contractual freedom. This choice is often then made at a wider—community—level, if and where the alternative tokens circulate with a more or a less wide acceptance.[15]

---

[13] This system has thus been defined as 'partially anonymous'; See Reuben Grindberg, "Bitcoin: An Innovative Alternative Digital Currency", 164.

[14] See Giulia Arangüena, "Bitcoin: una sfida per policymakers e regolatori", in *Diritto mercato tecnologia*,

Quaderno Anno IV, n.1 (2014): 23; Reuben Grindberg, "Bitcoin: An Innovative Alternative Digital Currency", 168.

[15] A particularly 'famous' complementary currency, *ex multis*, that is currently adopted at a local level and has reached an interestingly high level of circulation is the 'Bristol Pound'; this money can even be used to pay local taxes. For an overview on the functioning of this complementary currency, see http://bristolpound.org/.

For an overview of American case law dealing with complementary currencies, see Reuben Grindberg "Bitcoin: An Innovative Alternative Digital Currency", 182 ff.; see also Nicolei

Regulators, historically, seem to have become concerned with complementary currencies only when their circulation became so diffuse, that they constituted a threat to the official currency. This is where some restrictive or prohibitive rules can be registered. However, until complementary currencies do not expand to a level of "alert" for the government, who fears a loss on the control of its monetary policy, a certain leeway may be allowed, using the legal stratagem of barter, or payment by *datio in solutum* and so forth.

This allows for the extension by analogy of a "minimum" set of rules to solve some of the controversies that may arise from the use of Bitcoins, and more specifically, the rules on contract (given the consensual nature at the basis of the use of "alternative" currencies).

Applicable rules may include: those on formation and interpretation of contracts (where it may be necessary to determine which legal value the parties intend to attribute to the payment using an alternative currency); those on performance (where the timeliness of the payment or its exactness need to be assessed); those on breach of contract and contractual liability (including, *inter alia*, cases in which a party has tendered a token that is not a proper unit of the agreed upon currency of payment; or cases, in which the rules on breach of contract have been applied to the duties of the owners or managers of platforms where the tokens are stored).[16]

Whilst this may be a first important set of existing legal tools that may find application in controversies and litigation surrounding virtual currencies, it proves useless when some of the most problematic issues related to the use of Bitcoins arise, such as, for example, problems of fraud or bankruptcy (which may, and often do, also imply relevant issues

---

M. Kaplanov, "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation", *Temple University Legal Studies Research Paper*, 2012, (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203) (viewed July 2015).

[16] This was the legal claim (breach of contract) brought forth in 2012 by some users of Bitcoins who had been robbed of their virtual wallets stored on the Bitcoinica platform following a hacker attack. The users claimed that Bitcoinica had breached its contractual duties in not ensuring sufficient safety measures against hacking (See https://docs.google.com/file/d/0B_ECG6JRZs-7dTZ5QS0xcUkxQjQ/edit?pli=1) (viewed October 2015).

for criminal law).[17] The fact that Bitcoins escape from any supervisory or prudential control that would be useful in these hypotheses, explains the concerns on the systemic risks that may arise from the use of these instruments.

Virtual Currencies and Payment Services

The qualification of "complementary currencies" as "payment instruments" may allow, instead, for the extension of another set of important (existing) rules to Bitcoins: those on non-cash payments. The closest analogy that seems applicable is with the rules on transfers of funds (whereas rules on card payments or cheques do not seem applicable), at least as far as the need to determine the moment in which payment is considered as having been performed and the issue of whether or not a payment may be reversed if made by mistake or to the wrong beneficiary.[18]

However, the analogy cannot, at the moment and prima facie, be extended so far as to include payments in Bitcoins as falling within the notion of payment services as defined by the existing Payment Services Directive of the European Union.[19] Indeed, given that according to article 3, letter (l) of the Directive electronic money is excluded from its sphere of application, it would seem a fortiori to extend by analogy its application to virtual currencies (and all the more so, considering that whilst emission of e-money is only permitted to authorized subjects, emission/

[17] The legal vacuum concerning the regulation of Bitcoins does not only refer to the monetary issues and to the private law ones. Criminal law has had to deal with different crimes carried out on virtual currency platforms (especially trade of a variety of illegal goods and services paid for in Bitcoins); the funding of illegal activities using Bitcoins; money laundering; fraud; theft of Bitcoins from a platform; seizure of Bitcoins in case a platform is 'shut down' (i.e. Silk Road in 2013) and the ensuing problem of disclosure of the names of the subjects who buy and sell/transfer these digital 'tokens' (UK, Australia and South Africa have approved specific *key disclosure laws* for this last hypothesis: the refusal to provide the cryptographical keys to the authorities can be a criminally pursued).

[18] Article 4 A of the U.C.C. in the USA, for example, in its transposition in many States has been formulated so as to extend its applicability beyond transfers made through the banking system, and so as to comprise payments made by 'other subjects' as well. See Rhys Bollen, "The Legal Status of Online Currencies: Are Bitcoins the Future?", *Journal of Banking and Finance Law and Practice* 24 (2013): 23–25.

[19] Directive 2007/64/EC of 13 November 2007 on payment services in the internal market, in *OJ* L319 of 5 December 2007, 1

mining of virtual currencies is totally unregulated).[20] The proposal for the PSD2[21] seems to leave some scope, however, where the broadening of the definition of "payment services", as laid down in article 4 of the proposal, so as to include notions such as "third party payment service provider" and "payment initiation service", may comprise some of the activities carried out on platforms for the exchange of virtual currencies.

The current exclusion from the sphere of application of the European rules on payment systems does not prevent a pragmatic trend that some recent judgements and decisions of regulators have expounded, in which they have taken into account the activity of conversion of fiat currencies to and from Bitcoins and have considered those as falling within the notion of the provision of a payment service.[22]

The two immediate consequences of this qualification are on the one side, that this service has to be authorized (and thus at least to some extent controlled by the Surveillance Authority), and on the other, that this qualification could lead to considering this activity as taxable for revenue purposes.[23]

---

[20] See also, ECB, *Virtual Currency Schemes*, 43.

[21] Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market, [final compromise text], 2 June 2015, (available at http://data.consilium.europa.eu/doc/document/ST-9336-2015-INIT/en/pdf).

[22] Such was the outcome of a judgement (diffusely quoted) given by the French Commercial Court of Creteil in 2011 (judgement of 6 December 2011) that considered the activity of conversion of real currencies into digital currencies and vice versa carried out on some platforms as the equivalent of the provision of a payment service; and that as such, the activity is subject to authorization and control by the Surveillance Authority.

A similar qualification was given in the document released by the US Financial Crimes Enforcement Network (FinCEN), (US Department of Treasury) in 2013 (available at http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html, viewed October 2015) as an interpretative guide on the applicability of the US Bank Secrecy Act to persons creating, obtaining, distributing and exchanging virtual currencies. According to the interpretation given by the FinCEN, the conversion between real and virtual currencies carried out on some platforms qualifies as an activity of money transmission and thus falls under the scope of the Bank Secrecy Act. Following the release of this document, one of the then largest platform operating in Bitcoins, Mt. Gox, requested and obtained a licence as a Money Service Business (thus undergoing anti-money laundering and anti-terrorism controls).

[23] An interesting position in this sense is the one taken by the German Federal Authority for the Supervision of the Financial Sector, the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), that in a recent Regulation from 2013 considered Bitcoins as 'units of account' included within financial instruments that serve as 'substitute money', and whose use for a commercial scope requires an authorization under the German banking law (the Kreditwesengesetz). See also Giulia Arangüena, "Bitcoin: una sfida per policymakers e regolatori", 21.

Before considering taxation issues (*infra* section on "Virtual Currencies and Taxation"), the problem of potentially qualifying some of the services related to Bitcoins as banking activity also requires a few brief observations.

The qualification of an activity as "banking", for the purpose of applying banking statutes, obviously depends on the definitions found in the single national laws. A common requirement concerns the "activity", often defined as entailing both a "collection of savings" and an "issuance of credit". Whereas the first may be encountered in activities surrounding Bitcoins (and their potential qualification as investment instruments or financial commodities is closely tied to this issue, as will be seen *infra*), the second (issuance of loans) does not quite yet seem to be implemented. Regulators are thus left with the difficult choice of leaving "services" related to Bitcoins as totally falling beyond the scope of banking legislation, or trying to regulate at least some aspects of it—this is the examined case of the conversion activity, which is growingly qualified as requiring some form of authorization.[24]

The utility of extending banking laws to activities of emission and or conversion of Bitcoins has also been highlighted not only with reference to the prudential controls, but also with reference to the guarantees (for example, deposit guarantee schemes) that could eventually be extended to deposits in virtual currencies. The absence of a regulated infrastructure at the moment renders the "collection of savings" a risky activity for users.

Bitcoins and Investment Contracts

The starting point for the question of whether Bitcoins may qualify as "investment contracts" depends on the use of these tokens as a potential "store of value" examined earlier. Recognizing Bitcoins as investment

[24] Such is not only the outcome of the quoted FinCEN document, it is also, indirectly, the possible outcome of other documents: i.e. the Bank of Italy recently issued a Communication (Banca d'Italia, "Avvertenza sull'utilizzo delle cosiddette 'valute virtuali'" of 30 January 2015) according to which, while the private use and acceptance of virtual currencies in payment for goods and services are legal activities, the emission and conversion of virtual currency schemes without authorization may be sanctioned as a violation of the statutes that reserve banking activities and payment service activities only to authorized subjects (see articles 130, 131, 131-*ter* of the Testo unico bancario (d.lgs. n. 385/93) and article 166 of the Testo unico delle disposizioni in materia di intermediazione finanziaria (d.lgs. n. 58/98)).

contracts obviously depends on the national rules defining what constitutes investment contracts or instruments (in the absence, currently, of a relevant supranational legislation on the point—both the MiFID and the MiFID2, for example, do not seem to allow for the inclusion of virtual currencies within their sphere of application).[25]

The exclusion of the Bitcoins and other digital currencies from the category of investment contracts (where this is the regulatory choice) does not, however, constitute an obstacle to considering the activity carried out by some specific subjects in relation to digital currencies as potentially falling under prudential or supervisory regulation.[26]

In other legal systems, virtual currencies may be classifiable under the general notion of "payment instruments" and this enables the ensuing legislation to be applicable to these instruments, including Bitcoins.[27] Given the "investment" or potentially "speculative" use of Bitcoins that can be made by some operators, other systems are prone to considering them as "commodities" or "financial commodities"[28]; this is especially true where the concerns are related to taxing the "profit" arising from this investment instrument and thus this qualification or assimilation has been made by internal revenue authorities (see below).

---

[25] The Italian legislation for example excludes Bitcoins from the category of 'financial instruments' (see d.lgs n. 58/1998 (Testo unico delle disposizioni in materia di intermediazione finanziaria) at article 1-*bis*, 2nd comma and article 1-*bis* 4th comma, excluding means of payment from the notion of 'investment instruments' and excluding any instrument, not explicitly enumerated, within the notion of 'financial products' and sphere of application of the law (article 1, 1st comma, letter u)). This entails that the whole 'MiFID system' (as set down by Directive 2004/39/EC of 21 April 2004 on Markets in Financial Instruments in *OJ* L 145, 30 April 2004, p. 1 and by Directive 2014/65/EU of 15 May 2014 on markets in financial instruments (so-called MiFID2) in *OJ* L 173 of 12 June 2014, p. 349) will also be inapplicable to virtual currencies.

[26] See footnote 24 quoting the Document released by the US FinCEN and the Communication by the Bank of Italy.

[27] For example, Bitcoins could be considered as 'financial products' under the Australian Corporations Act 2001 when considering them as 'a facility' through which non-cash payments are made. See Bollen, "The Legal Status of Online Currencies: Are Bitcoins the Future?", 20.

See also footnote 9 for references on recent US case law.

[28] The Governments of Japan and Finland have officially classified Bitcoins as a commodity. The Internal Revenue Service of the United States in 2014 declared that Bitcoins, for the sole purpose of taxation, can be assimilated to property. Thus revenue taxes for US citizens on operations using Bitcoins will be applied with reference to the date of the operation. See Giulia Arangüena, "Bitcoin: una sfida per policymakers e regolatori", 21; Maria Letizia Perugini, Cesare Maioli, "*Bitcoin*: tra moneta virtuale e *commodity* finanziaria", available on http://ssrn.com/abstract=2526207, 10 ff and 1.

Virtual Currencies and Taxation

The issue relating to the definition of the legal nature of virtual currencies is closely tied to another aspect: the possibility of taxing revenues in Bitcoins.[29] Whereas an initial trend seemed to completely ignore revenues in virtual currencies and, more generally, "virtual assets", in what was defined as an attitude belonging to the wider phenomenon of non-understanding on behalf of the legislator of the so-called "virtual economy" that escapes any form of public regulation, including, for example, taxation,[30] the current trend seems to have changed.

Recent important positions taken by some legislators and/or taxation and revenue authorities must be recalled. They all imply a two-step process: defining the nature of Bitcoins and then verifying if they fall within a category of taxable assets. As quoted above, this is the position taken by the Internal Revenue Service of the United States, which recently declared that Bitcoins, for the sole purpose of taxation, can be assimilated to property. The Canada Revenue Agency has also declared in 2013 that it will tax Bitcoins under two headings: transactions for goods and services will be taxed under its barter transaction rules, and profits made on commodity transactions could be income capital under its transactions in securities.[31] In 2014, the Brazilian tax authority also took a position that seems in line with the definition given by the US Internal Revenue Service: the Receita Federal considers digital currencies as financial assets that are subject to taxation (although only if possessed above a certain threshold value, thus exempting small consumer purchases).[32]

The European Court of Justice has also very recently considered the issue in the case *Skatteverket* v. *David Hedqvist*.[33] The judgement, concerning whether the operations of conversion between real and virtual currencies are subject to the common value added tax (VAT) or are

[29] For more details on taxation and Bitcoins, see Chap. 10 in this book.

[30] See for example, on taxation of 'virtual property' acquired on online games, Leandra Lederman, "'Stranger than Fiction': Taxing Virtual Worlds", in 82 *NYU Law Review* 1620, 2007.

[31] See Section 3 on Barter transactions and Section 39 on Transactions in securities of the Canada Revenue Agency Interpretation Bulletin.

[32] Taxation of gains on Bitcoins would fall under the scope of article 55, inciso IV of the Regulamento do Imposto de Renda de 1999.

[33] Case C-264/14 of 22 October 2015.

exempt from it (according to article 135 (1) of the Directive 2006/112/EC),[34] is worth quoting for two reasons.

On the one hand, with reference to the issue of taxation, the European Court of Justice holds the activity of conversion as falling within the notion of supply of services for consideration (as defined in article 2 (1) of the Directive) but considers it exempt from the VAT because it falls under article 135(1)(e) which exempts transactions involving, *inter alia*, "currency [and] bank notes and coins used as legal tender".

On the other hand, the court also gives an incidental definition on the nature of Bitcoins: "currencies other than those that are legal tender in one or more countries, in so far as those currencies have been accepted by the parties to a transaction as an alternative to legal tender and have no purpose other than to be a means of payment, are financial transactions". […] It is common ground that the "bitcoin virtual currency has no other purpose than to be a means of payment …".[35] The court further adds that Bitcoins cannot be considered as securities.[36]

Challenges for the Regulator

As the brief considerations above suggest, there is a legal vacuum that can be bridged with the existing rules only to a certain extent and not always with satisfactory results. There may be, for example, also a "danger" in use of analogy to extend application of norms without having provided the necessary supervision or authorization: a sort of free rider mechanism for miners and creators of digital currencies who confide in the "confidence effect" that regulated banking and payment systems may have on the public, without there having been any control and especially because there is no central authority that can serve as a lender of the last resort.[37]

The quest for "regulation" has been voiced by different actors. If and how this regulation should be tailored remains a challenging issue.

---

[34] Directive 2006/112/EC of 28 November 2006 on the common system of value added tax in *OJ* L 347 11 December 2006, 1.

[35] European Court of Justice, *Skatteverket* v. *David Hedqvist*.

[36] And thus transactions in Bitcoins do not fall within the scope of the exemption from VAT laid down in article 135(1)(f) of the Directive for transactions in securities.

[37] A risk highlighted, *inter alia*, by the EBA in its *Opinion on Virtual Currencies*, 44.

Whereas "currencies" are traditionally the domain of national rules—a symbol of monetary sovereignty—the characteristics and problems and risks posed by virtual currencies go beyond the notion of legal tender and are by their very vocation transnational. This may be a valid reason to hope that at least in the European area, and especially within the European Economic and Monetary Union, a regulation be adopted at Community level.[38]

A second set of problems concerns the moment (*ex ante* or *ex post*) in which regulation should intervene and its stringency.[39]

As far as the temporal aspect is concerned, in some cases an *ex post* regulation may be particularly useful. Such is the case with PayPal, for example, where a banking authorization was granted in Luxembourg in 2007 after the system was widely used and had gained the confidence of users (thus a legal intervention on an instrument that, based by its very nature on the trust of its users, has proved to be able to "survive" on the market).

The issue of the "stringency" of legislation is problematic if one considers the risks of an excessively detailed regulation, that may very rapidly become technically obsolete, given the digital nature of Bitcoins and virtual currencies and their rapid evolution.

In the meantime, the steps taken by some internal agencies (banking authorities, financial crimes enforcement agencies, internal revenue agencies, and courts) seem to point in two directions: either qualifying these activities as "para-banking" activities (which may become especially relevant if and when Bitcoins will also be used for loans), thus entailing that activities related to conversion and emission of Bitcoins have to be authorized under national banking laws; or considering them as "payment services", that have to be authorized under those specific laws. It does not seem that legal systems are prone to recognizing digital currencies as legal tender anywhere, though they may be "allowed" or "recognized" as units of account or as complementary currencies.

---

[38] The interest of the European market in this sense is quite evident, as demonstrated by the studies carried out by the ECB and the EBA which focus especially on the problem of the risks associated with the use of digital currencies.

[39] See, for example, the potential and (limited) instruments of intervention at the disposal of the IMF in case of a speculative attack by a private digital currency against the value of a real currency, Nicholas A. Plassaras, "Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF", *Chicago Journal of International Law* 14 (2013): 377.

References

Ametrano, F. M. *Hayek money: The cryptocurrency price stability solution*. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270

Arangüena, G. (2014). Bitcoin: una sfida per policymakers e regolatori. *Diritto mercato tecnologia,* Quaderno Anno *IV*(1), 19–43.

Bollen, R. (2013). The legal status of online currencies: Are Bitcoins the future? *Journal of Banking and Finance Law and Practice, 24*, 272–293.

European Banking Authority (EBA). (2014, July). *Opinion on* '*virtual currencies*'. Reterived from https://www.eba.europa.eu/documents/10180/657547/EBA-Op-201408+Opinion+on+Virtual+Currencies.pdf

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

Financial Action Task Force. (2014, June). *Virtual currencies. Key definitions and potential AML/CFT risks*. Reterived from http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Grindberg, R. (2012). Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal, 4*, 160–208.

Kaplanov, N. M. (2012). *Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation*. Temple University Legal Studies Research Paper. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203

Law Library of Congress. *Regulation of Bitcoin in selected jurisdictions*. http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

Lederman, L. (2007). 'Stranger than fiction': Taxing virtual worlds. *NYU Law Review, 82*, 1621–1672.

Nakamoto, S. *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Perugini, M. L., & Maioli, C. *Bitcoin*: tra moneta virtuale e *commodity* finanziaria. Available on http://ssrn.com/abstract=2526207

Plassaras, N. A. (2013). Regulating digital currencies: Bringing Bitcoin within the reach of the IMF. *Chicago Journal of International Law, 14*, 377–407.

Yermack, D. (2013, December). *Is Bitcoin a real currency? An economic appraisal*. NBER Working Paper No. 19747.

4

Mobilizing Payments Within the European Union Framework: A Legal Analysis

Gabriella Gimigliano

Abstract Gimigliano examines mobile payment services within the European Union framework. In the European Union, policymakers are developing a process of integration to build up a single payment area. This process is based on self-regulation under the umbrella of the European Payment Council and the institutional sources of law, such as Directives and Regulations. Both actions promote interoperability among stakeholder standards, financial stability and fund customer protection. To this end, it is critical to ascertain to what extent Community-based rules and regulations on payment services and electronic money may also be applicable to mobile payments.

G. Gimigliano (✉)
Lecturer in Business Law, Department of Business and Law, University of Siena, Italy

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_4

Introduction

Mobile devices and mobile payments (henceforth referred to as m-payments) have been studied recently as a means of financial inclusion by leading international regulators and financial supervisors.[1]

According to the 2015 Consultative Report, co-authored by the Committee on Payment and Market Infrastructure at the Bank for International Settlements and The World Bank Group, the objective of financial inclusion should be pursued so that all individuals and micro-enterprises can be provided with at least one transaction account. Transaction accounts will allow account holders to make and receive payments and store money value. In fact, the access to payment services is regarded as an important part of the overall package of financial services.

However, the studies carried out revealed direct and indirect factors influencing the de facto choices of unbanked and underbanked people. Such factors range from high fees for access to, and maintenance of, transaction accounts, costs of transportation to the next branch or point of service, especially in rural areas, and the low level of financial literacy as well as the state of economic and labour "informality". Additionally, the report underlined the lack of attention to cultural and religious diversity, scarce payment product design and the perception of unsafe service providers.[2]

The goal of financial inclusion is also threatened by the lack of a business case for service providers. In fact, unbanked and underbanked people have, most of the time, irregular incomes or small value incomes, while payment service providers have to meet a set of fixed costs, such as anti-money laundering requirements or "know your customer" rules, costs which are difficult to recover.[3]

Within the above framework, mobile devices are regarded as a viable alternative to the traditional access to the payment system. In fact, m-payment services emerge as a large potential market and, as a rule of

[1] M-payments together with e-money products and basic transaction accounts have generally been treated as a means of financial inclusion.

[2] CPMI and The World Bank Group, Consultative Report. Payment Aspects of Financial Inclusion, September 2015.

[3] See CPSS, Innovations in retail payments, May 2012.

thumb,[4] they may turn out to be a suitable tool for lowering access and processing costs of payment transactions for both users and providers.

However, the higher risk level is an issue. Accordingly, a 2014 International Monetary Fund study established operational resiliency, financial integrity and safeguarding customers' funds as oversight priorities for m-payments. Apart from operational and liquidity risks, the bankruptcy of m-payment providers and the m-payment infrastructure may drag down the reputation of the payment system as a whole.

Despite the higher level of risk, it is widely recognized at international level that these m-payments do not pose a new type of risk. Rather, the proper functioning of the payment system and the stability of the financial system are threatened by the new design of the payment system: "the more contact points there are between the networks and the users and the more complex is their functioning, the more challenging is risk control".[5]

In this regard, the widespread enforcement of bank-based requirements to non-bank m-payment providers has been proposed as a workable legislative solution. However, the Community-based regulatory experience on e-money and e-money institutions has revealed how such a solution is likely to cramp innovation and competition.

This chapter aims to critically investigate m-payments within the Community-based legal framework.

The chapter will, firstly, provide an overview of the main achievements of self-regulatory activity and, secondly, establish to what extent the institutional framework—namely the European rules and regulations for banks, e-money institutions and payment institutions—is applicable.

This chapter contains three further sections. The next section covers the self-regulatory approach, examining the early results of cooperation among financial intermediaries and their associations on the one hand, and the European Payment Council (EPC) on the other. The penultimate section turns to the institutional framework investigating m-payments in

[4] See Chap. 6.

[5] Terry Bradford, Fumiko Hayashi, Christian Hung, Simonetta Rosati, Richard J. Sullivan, Zhu Wang, and Stuart E. Weiner, "Nonbanks and Risk in Retail Payments: EU and U.S.", edited by M. Eric Johnson, *Managing Information Risk and the Economics of Security* (Berlin: Springer 2009), pp. 17–53.

comparison with the notion of "payment service" and "e-money", while the final section draws conclusions from the main results of the analysis.

The Self-Regulatory Approach and the Business Models

Thanks to the self-regulation carried out under the umbrella of the EPC, two preliminary results have been achieved: firstly, a definition of m-payments was established, and secondly, three main m-payment business models were outlined, and this helps give an overview of the m-payment ecosystem's stakeholders and m-payment chain.

According to the SEPA guidelines, the concept of m-payment includes any transfer of funds initiated through a mobile device. It is essential to establish a definition of m-payment, because there is no legislative definition within the European framework and, in turn, the economic literature tends to swing between more flexible and stricter definitions.

As for the business models, the 2010, 2012 and 2014 White Papers pointed to proximity or contactless m-payments, remote m-payments and mobile wallets blending contactless and remote systems.[6]

They share the following features:

- They have no value ceiling;
- They represent new forms for entering the payment system but are based on traditional means of payment: card payments, credit transfers and, sometimes, direct debit;
- They state that the m-payment user must have already downloaded an application to make his or her mobile device suitable for m-payments and have already made a contract with a payment service provider to enable him or her to transfer funds through mobile devices.

However, according to the SEPA general principles, not every means of payment is suitable for every kind of m-payment business model and for every party to a payment transaction.

[6] See Chap. 2 for further information on contactless and remote payments as well as on m-wallets.

Indeed, mobile contactless business models are mainly consumer-to-business transactions and are traditionally card based.[7]

In 2012, the second EPC White Paper envisaged mobile card payments to provide business-to-business and business-to-consumer payment transfers, but such labels are to some extent deceptive.[8] Indeed, as the 2012 White Paper emphasizes, most of the business-to-consumer payment transactions are refunds initiated by the consumer to send the payment account identifier to the merchant, while in business-to-business m-payment transactions the payer is actually acting as a consumer but the White Paper gives no further explanation.

In addition, the 2012 EPC White Paper expressly excluded mobile direct debit contactless payments because this means of payment is initiated by the payee, while contactless credit transfer payments are contemplated, applying a hybrid technological model. For example, when a transport ticket is renewed, the payment is initiated as a contactless m-payment, swiping a mobile device at a point of sale, but the funds order is authorized remotely.

Turning now to remote m-payments,[9] the SEPA principles are based on card payments and credit transfers, even though direct debit m-payments are not expressly excluded. The basic schemes cover business-to-business, consumer-to-business and consumer-to-consumer payment transactions. Apart from the means of payment used and the status of payer and payee, remote m-payments mostly follow the same set pattern[10] and this, above all, implies that the beneficiaries ask for some form of instant or near-instant confirmation of payment or payment execution certainty.[11]

---

[7] In fact, when a purchase agreement is made (or the service agreement is made), the trader will enter the transaction amount on the POS (namely, point of sale) terminal and the payment transaction is confirmed by tapping the mobile device on the terminal: the payment transaction is performed through the default payment card. This type of m-payment may also require a double-tap and the use of a personal code to confirm the payment order. Moreover, the 2012 EPC White Paper outlined a more ambitious plan: setting out consumer-to-consumer card-based m-payments.

[8] Consumer-to-consumer SEPA contactless m-payment transactions are not being applied as yet. They are based on the participation of the payment card scheme.

[9] See Chap. 2.

[10] Compare: EPC, White Paper. Mobile Payments, 18 October 2012, p. 30 ff.

[11] See EPC, White Paper. Mobile Payments, 18 October 2012, p. 44 ff.

Finally, the 2014 EPC White Paper on Mobile Wallet Payments set out the idea of a digital wallet that allows the holder to "access, manage and use mobile payment services, possibly alongside non-payment applications", such as information relating to identity cards or digital signatures and certificates.[12]

Apart from the distinction between horizontal and vertical mobile wallets as well as m-wallets hosted by the wallet holder on a commercial website or on a secure server, what sounds more interesting is that customers should be allowed to make their payments throughout the European Union by means of their mobile wallet according to the principle of irrelevance of the country of origin of the fund transfer orders and mobile wallet issuance.

In the end, the analysis of SEPA-based mobile business models shows that:

- The "ecosystem" of m-payments is made up of various natural and legal entities and most of them do not belong to the financial system. In fact, the players involved are not only the payee (consumers or merchants), the payment service providers and the clearing and settlement bodies, but also some others such as the secure element (SE) issuer, the mobile network operator (MNO) responsible for securely routing messages, operating the mobile network, issuing and recycling mobile phone numbers, and the payment gateway provider, namely a trusted third party acting on behalf of the SE issuer and/or the m-payment service issuers to facilitate an open system. This list is far from being closed. Such an "ecosystem" naturally raises the issue of regulatory consistency between the sources of law applied. In legal terms, the critical point is how to allocate responsibility among them for the execution of the payment transaction. This issue is all the more critical when the MNO enters into an agency or outsourcing agreement with the payment service provider;
- The above-mentioned m-payment transactions are based upon a transaction account or, in other words, a contract has been made

[12] EPC, White Paper. Mobile Wallet Payments, January 2014, p. 16.

between a user and a financial institution, either by credit, payment or electronic institutions. This means that telcos and MNOs perform only the task of data carrier and, therefore, the institutional framework for payment service providers will be regularly applied. Reference is mainly, but not exclusively, made to the PSD, PSD2 and e-money directives;

– Alternatively, telcos and MNOs could enter the relevant market as a payment service provider and, accordingly, apply for authorization as a credit institution, payment institution or e-money institution, or indirectly by establishing a financial subsidiary within the EU;
– SEPA business models are based entirely upon traditional means of payment. This implies that, (i) SEPA rule books on credit transfers and direct debit, as well as SEPA standards on card-based payments are applied, and (ii) PSD (and PSD2) provisions on the rights and liabilities of the contracting parties, in particular on the authorization and the execution of payment transactions, are applied as well. Finally, SEPA principles leave any m-payments based entirely on MNOs outside the scope of self-regulatory activity. This is the case for telcos and MNOs that do not simply perform the task of data transporting, but allow their customer to use pre-paid balances for third-party payments too. Therefore, the "banks would be no longer involved in the consumer-to-merchant or in the consumer-to-consumer side of the payment."[13] One wonders whether telcos and MNOs should be authorized as credit institutions, payment institutions or e-money institutions. In addition, it should be established whether the Community-based institutional framework for payment services is to be applied to the payment services they provide.

In the following paragraph, the chapter investigates the European institutional framework for payment services, paying close attention both to

[13] Malte Krueger, "The Future of M-payments: Business Options and Policy Issues." Electronic Payment Systems Observatory, Institute for Prospective Technological Studies, Joint Research Center, European Commission, Report EUR 19934 EN, August 2001, 18. To download from epso.jrc.es/Docs/Backgrnd-2.pdf.

PSD and PSD2 being prepared for publication in the Official Journal of the European Communities. The goal is to ascertain whether m-payments may be subsumed under the concept of payment service and e-money when telcos and MNOs behave either as mere carriers or providers of third-party payments. Indeed, within the European institutional framework, the concepts of payment services and e-money are based upon rules and regulations aiming to protect customers' funds, the soundness of payment service providers and the proper functioning of the payment system.

The Institutional Framework for Payment Services

Payment services and electronic money (henceforth referred to as e-money) are two basic concepts upon which PSD, PSD2 and e-money directives are centred. To what extent can m-payments come under such headings?

M-Payments and Payment Services in the PSD

There is no Community-based definition for payment services. In fact payment services are described only as "any business activity listed in the Annex". According to the PSD Annex, the concept of payment services covers (i) any activities enabling cash to be paid into and withdrawn from a payment account, (ii) any activities based on a payment account that aim to execute payment transactions by means of direct debit, credit transfer and/or card-based payments, (iii) the activities of issuing and acquiring payment instruments and (iv) money remittance .[14] Apart from the technical differences, it seems that a payment service exists if the ser-

[14] PSD draws the difference between payment services and payment transactions. Both of them are referred under article 4: compare n. 3, 5 and the Annex.

vice provider professionally "enters into possession of the funds to be transferred"[15] for making a payment.

Indeed, laying down the negative scope of PSD, article 3, letter (j) provided that the directive is not applied to:

> Services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision and maintenance of terminals and devices used for payment services (article 3, letter (j)).

Drawing a comparison with m-payments as outlined in the SEPA-based principles, there is little doubt that these are payment services according to the concept mentioned above. In fact, PSD Annex (n. 7) on payment services expressly covers the:

> Execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

This means that, when telcos and MNOs perform a mere task of data transferral, the professional provision of payment services by mobile devices is a regulated activity. This activity can be performed only by entities that have been provided with a specific licence as credit institutions, e-money institutions or payment institutions.

Thanks to the principle of mutual recognition, the European licence enables the legal entity to provide the payment services throughout the Member States, either establishing a branch or providing services from abroad, and no further authorization may be required. However, the European licence is issued on condition that the entity meets a set of

[15] See Maria Chiara Malaguti, "The Payment Service Directive. Pitfalls between the Acquis Communautaire and National Implementation", ECRI Research Report 9 (2009): 11.

initial and ongoing requirements in terms of capital level, own funds and corporate organization. Moreover, the home State authority is entrusted with supervising sound and prudent management of the entity.

In this context, it is conceivable that the financial intermediaries will professionally provide m-payments, while telcos and MNOs intervene as agents or as outsourcees in one or more steps of the payment chain. In this way, the payment service providers take on all the risks. Indeed, the payment service provider is fully liable for the regular and correct execution of payment services (for example, see article 17 and 18 PSD).

A slightly different situation exists when a mobile operator acting as an intermediary between the financial institution and the user is the only entity the user deals with. This happens when a mobile operator holds a payment account with a bank in its name but on behalf of each and all of its customers and through which customers' payment transactions are processed. Here, again, the mobile operator might act as a mere agent for the bank, but this depends, considering the above remarks, on who holds responsibility for the proper execution of payments and fund safety in the customer-provider relationship. If the mobile operator takes on this responsibility, the mobile operator is actually acting as a payment service provider and should have the necessary licence; on the other hand, if the responsibilities are taken by the bank, the mobile operator is acting as an agent of the bank.[16]

Furthermore, telcos and MNOs might consider the possibility of entering the relevant market either as "pure" or as "hybrid" payment institutions.

The payment institutions are the financial intermediaries specialized in the provision of payment services as laid down in the PSD Annex. However, they have less cumbersome requirements in terms of organization, capital and own funds compared with credit institutions. Indeed, the main objective pursued at Community Law level was to lay down a risk-based regulation. The payment institution set up would become a subsidiary of one or more telcos and MNOs taking advantage of their wide customer base.

[16] Compare: The World Bank, From Remittance to M-Payments", October 2012, 3 and Maria Chiara Malaguti, "The Payment services Directive. Pitfalls between the Acquis Communautaire and National Implementation", ECRI Research Report 9 (2009): 18.

European authorization for payment institutions enables them to provide not only m-payments and the other payment services listed in the Annex, but also to operate closely related activities and payment systems. In addition, the payment institutions are authorized to provide both single payment transactions and payment accounts services, as well as to extend a line of credit, provided that the credit is granted for a limited period of time and in connection with a payment to be carried out.

"Hybrid" payment institutions are "in-between" entities. These entities are engaged in both the provision of payment services and in non-financial business. This is the case of telcos and MNOs that plan to bridge the gap between the two markets.

The so-called hybrid payment institutions are legal persons with a proper licence but the competent authorities may (article 10.5 PSD):

> Require the establishment of a separate entity for the payment services business, where the non-payment services activities of the payment institution impair or are likely to impair either the financial soundness of the payment institution or the ability of the competent authorities to monitor the payment institution's compliance with all obligations laid down by this Directive.

Like "pure" payment institutions, they are authorized to provide the payment services listed in the Annex, perform complementary activities such as the operation of payment systems and extend credit for a limited period of time by using funds other than user funds, with the exclusive aim of executing payments.

However, the harmonized framework suffers from a set of heterogeneous exemptions. Such exemptions turn out to be of some interest to the m-payments framework too. Apart from the general exemptions based either on the lack of any direct or indirect relationship between the service provider and the final user (article 3, letter (n)) or the business volume of the service provider (article 26 PSD), a very interesting exemption is set out in article 3, letter (i):

> Payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided

> that the telecommunication, digital or IT operator does not act as an intermediary between the payment service user and the supplier of the goods and services (article 3, letter (l)).

Here, a reference is made to markets others than the market for payment services. Indeed, this exemption covers those instances in which the digital goods and services, such as music, newspapers, or ring tones, are produced either by a third party or by the mobile operator, but the latter may "add intrinsic value to them in the form of access, distribution or search facilities." (preamble (6) PSD).

M-Payments and Payment Services in the (*forthcoming*) PSD2

The revised PSD, according to the text published last October, has laid down a wider concept of payment services. Namely, the idea of payment services is no longer based exclusively upon the user funds possessed (funds to be used to make payments), but also on access to payment account data.

The European policymaker is following the technological development of the payment system and that has led to the payment chain becoming heavily fragmented.

Within this context, PSD2 has provided an interesting new payment service in the Annex, among others, called the "payment initiation service". This means that this professional activity must be carried out with the necessary authorization, but a softer set of licensing requirements has been set out in compliance with a risk-based regulatory approach. Namely, the draft PSD2 establishes that the providers of payment initiation services must hold a professional indemnity insurance or equivalent covering the territories and must take on the responsibility for late, unexecuted or defective execution of the payment order with regard to their own place in the payment chain.

It should be considered a pro-competitive aspect of the new framework. The payment initiation service provider can operate its services with the consent of the account holder also without making an agreement with

the "servicing payment service provider" account on the specific business model to be used for the provision of the payment initiation services.

The area of exemptions as laid down in the PSD negative scope provision has been improved but not extensively modified.

M-Payments and the E-Money

Turning now to the concept of e-money, firstly the 2000 directives and then the 2009/110/EC directive set out a definition of e-money. They established that e-money is the result of a process of exchange from bank-based money as well as coins and notes to an electronically "stored monetary value" conferring on the holder a claim over the issuer. E-money products must meet the following requirements:

- the process of conversion must be "reversible", namely, "upon request by the electronic money holder, electronic money issuers redeem, at any moment and at par value, the monetary value of the electronic money held."
- being accepted as a means of payment by natural or legal person other than the issuer,
- being issued for the value of the funds exchanged or less.

The point is the following: when mobile operators allow their customers to make payments, and the same mechanism is used as when the client buys airtime, are they issuing e-money according to the above-explained definition? Should they therefore, be authorized as e-money institutions?

This is a critical issue. Indeed, issuing e-money is a regulated activity and may be carried out only by the properly authorized legal entities. Authorization enables these institutions to operate their business, with or without a branch, throughout the European Union according to the European principles of the single licence and home country control. However, the authorization process compels a legal entity to meet a set of legislative and regulatory requirements, basically comparable to those laid down for payment institutions and they are subject to prudential supervision (preamble n. 9, 2009/110/EC Directive.).

The 2009/110/EC directive also defines the scope of e-money institutions. In addition to issuing e-money, the e-money institutions may also be authorized to provide payment services in compliance with the specific framework, either as a "pure" or as a "hybrid" institution.[17]

To make a choice, one might consider the way in which the clearing and settlement activities are carried out.

One might assume that the mobile operator opens a pooling account with a bank in its own name on behalf of the users where the funds received by the customers to make the payments are stored. Therefore, the mobile operator becomes a trustee of the customers. In this case, the clearing and settlement activities are performed through the banking system.

Alternatively, one might assume that the mobile operator operates a closed-loop system and peer-to-peer payment transactions, performing the clearing and settlement activities with no connection with the banking system.

However, the issue of who is responsible for the clearing and settlement activities is not as persuasive an argument as it seems to be. Indeed, also conventional e-money institutions usually take part indirectly in the clearing and settlement structures, through credit institutions.

The main point at issue is whether the pre-paid balances, already used for buying airtime, can be considered as e-money under the definition set in the 2009/110/EC directive.

Considering them both, the redeemability of e-money seems to be the distinguishing feature. In fact, unlike e-money does, mobile pre-paid balances are not per se wholly or partially redeemable at par value and at any time, upon request by the holder when redemption is requested before the expiry of the contract.

Lastly, the application of the e-money directive to m-payments is strongly influenced by the established list of exemptions.

In addition to the general exemption based on the average amount of e-money outstanding, there also is a specific exemption. Like PSD, the e-money directive exempts from the institutional framework for e-money institutions any instance in which electronic monetary value is used to

[17] With regard to "hybrid" entities, see, art. 16 PSD.

purchase digital goods or services, and "by virtue of the nature of the goods or services" the telcos and MNOs "add intrinsic value to it". This extra-value may be represented by access, search or distribution facilities given that the goods to be bought or the services to be enjoyed can only be used by a digital device, such as mobile devices. Thus, even if the user has no direct or indirect relationship with the supplier, and the funds for payment of the price of the service are received from the MNO, the MNO is deemed not to perform a merely intermediary function. In fact, the product is something more than a payment transaction and belongs to a different market.

Conclusions

Drawing conclusions, this analysis has underlined the positive synergy between self-regulation and the institutional legislative actions.

Concerning self-regulation, the EPC is entrusted with carrying out a tricky task within the SEPA, namely, to reach an agreement on m-payment schemes in order to provide, in the future, a set of regulatory and technical standards. As underlined at the international level, the standardization process can bring about an increase in the level of interoperability and this can, in turn, pave the way for a more competitive context. However, the protection of customers' data and funds as well as the soundness of the financial system fall outside the main objectives of efforts at self-regulation.

Coming back to the institutional framework, joint analysis of the PSD, the draft PSD2 and the e-money directive has outlined how the concepts of payment services and e-money can be considered the benchmark for the regulation of m-payments within the EU framework. The European policymaker is trying to manage the technological fragmentation of the payment chain. Indeed, the concept of "payment service" has gone beyond being simply a matter of possessing users' funds to cover also the mere possession of user data for payment accounts. Might this change improve the "effet utile" of the EU framework? Wider protection can spur the financial inclusion process, but it needs to be traded off with a set of regulatory exemptions which rarely achieve great consistency.

References

Committee on Payments and Market Infrastrcuture (CPMI), The World Bank Group. (2015, September). *Consultative report. Payment aspects of financial inclusion*. 1–77. Retrieved from http://www.bis.org/cpmi/publ/d133.pdf

Committee on Payments Settlement Systems (CPSS). (2012, May). *Innovations in retail payments*. 1–96. Retrieved from http://www.bis.org/cpmi/publ/d102.htm

European Payment Council. (2012, October 18th). *White Paper. Mobile payments*.

European Payment Council. (2014, January). *White Paper. Mobile wallet payments*.

Krueger, M. (2001). *The future of M-payments: Business options and policy issues*. Electronic Payment Systems Observatory, Institute for Prospective Technological Studies, Joint Research Center, European Commission, Report EUR 19934 EN, August 2001, 1–24. To download from epso.jrc.es/Docs/Backgrnd-2.pdf

Malaguti, M. C. (2009). The payment services directive. Pitfalls between the Acquis communautaire and national implementation. *ECRI Research Report, 9*, 1–32.

The World Bank. (2012, October). *From remittance to M-payments*. 1–20. Retrieved from http://siteresources.worldbank.org/EXTPAYMENTREMMITTANCE/Resources/WB2012_Mobile_Payments.pdf

Vandezande, N. (2013). Mobile wallets and virtual alternative currencies under the EU legal framework on electronic payments. *ICRI Working Papers, 16*, 1–28.

5

A Fuzzy Set in the Legal Domain: Bitcoins According to US Legal Formants

Andrea Borroni

Abstract Reviews and journals are currently revolving the topic of cryptocurrencies, even if, so far, the domain of law has not found the spur to adequately and univocally frame this phenomenon. Nonetheless, the US legal theory is presently debating how to include Bitcoins into pre-existing "regulatory folders", while the country's judiciary is dealing with the first cases pertaining to Bitcoins. The reaction of the US legal system to this radical technological innovation demonstrates that the operational rules resulting from the joint action of the legal formants may grant a legal system a first response by relying merely on its own legal tools. In light of this, the present article investigates the reactions to Bitcoin and the potentially suitable regulatory frameworks proposed by US legal theory.

A. Borroni (✉)
Tenured researcher, "Jean Monnet", Department of Political Sciences, Second University of Naples, Italy

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_5

Introduction

Bitcoins are generally defined as a cryptocurrency: namely, an online, decentralized, stateless means of payment, which is based on a peer-to-peer network through which users can sell, purchase and exchange their units. The main advantage offered by this digital resource lies in the lack of third party intermediaries (such as credit and financial institutions) or central authorities, which consequently results in the absence of the usual transaction costs.[1] Besides, Bitcoin is commonly regarded as a potentially anonymous means of payment, since users are identified by "Bitcoin addresses" only,[2] even though, the peer-to-peer network is so designed to keep records of all transactions within the system and with the Bitcoin exchanges.[3]

Hence, given the specific structure of the Bitcoin system, coupled with its rapid spread throughout the world, Bitcoin is now a global phenomenon. Its advent, however, has destabilized the traditional patterns concerning state regulatory action, taxation, licensing, and so on, raising also a number of new legal issues.[4]

In light of this, this essay aims at analysing how countries around the globe have reacted to the present phenomenon, with a specific focus on the current debate in the USA.

---

[1] For a detailed description of the system and its functioning, see the original paper of Bitcoins' developer, S. Nakamoto, namely, Satoshi Nakamoto, *Bitcoin*: *A Peer-to-Peer Electronic Cash System* (2009), *available at* http://www.bitcoin.org/bitcoin.pdf.

[2] Joshua J. Doguet, "The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System", *Louisiana L. Rev*. 73, no. 4 (2013): 1119 ff. Jeffrey Alberts and Bert Fry, "Is Bitcoin a Security?", *B.U. J. Sci.* & *Tech. L.* 21, (2015): 1, 2–3.

[3] Benjamin Wallace, *The Rise and Fall of Bitcoin*, Wired Magazine (23 November 2011), *available at* www.wired.com/magazine/2011/11/mf_bitcoin/. Bitcoin exchanges, like BTC China or Bitfinex are online platforms through which users can purchase Bitcoins with traditional fiat currencies. For an overview of worldwide Bitcoin exchanges, see http://bitcoincharts.com/markets/.

[4] Examples thereof are: (i) the use of Bitcoins for criminal activities due to the anonymity of the peer-to-peer system; (ii) the threat Bitcoins pose to national sovereignty since they do not fall under the purview of domestic or international monetary policies (hence, they may become a sort of 'tax haven'); (iii) the lack of a central authority which prevents any potential intervention in case of excessive inflation or deflation; (iv) finally, no entity is in charge of establishing a uniform interest rate. Primavera De Filippi, "Bitcoin: A Regulatory Nightmare To A Libertarian Dream", in *Internet Policy Review* 3, no. 2 (2014), 2 ff.

Cryptocurrencies and Virtual Currencies

Presently, there are diverse cryptocurrencies which share basic features with Bitcoins, above all, the architecture, even if many of them allegedly offer better performances than Bitcoins based on the technological improvements which should make them faster, safer or simply more efficient.

Just to cite few examples, there are the so called alternative cryptocurrencies or "altcoins",[5] such as, Litecoin, GeistGeld, SolidCoin, BBQcoin, and PPCoin, (along with an amended version of the architecture of Bitcoins, named Bitcoin Two, which displays a higher degree of system anonymity), as well as virtual currencies which are not based on cryptography, like Liberty Reserve, WebMoney, Perfect Money, and CashU, which however require their users to "go through a third party to buy or sell their currency",[6] even though they are designed to be completely anonymous.

As regards specifically virtual currencies, according to the definition of the US Government Accountability Office (GAO), these are "digital unit[s] of exchange that [are] not backed by a government-issued legal tender. Virtual currencies can be used entirely within a virtual economy, or can be used in lieu of a government-issued currency to purchase goods and services in the real economy".[7]

An example of that is the Linden Dollar, used in a role-playing game, called Second Life, in order to virtually purchase goods and land and gain profit. The game supervises the use of the currency and also allows players

---

[5] Sarah Jane Hughes and Stephen T. Middlebrook, "Regulating Cryptocurrencies In The United States: Current Issues And Future Directions", *Wm. Mitchell L. Rev.* 40, (2014): 813. See Juliya Ziskina, "The Other Side of the Coin: The Fec's Move to Approve Cryptocurrency's Use and Deny Its Viability", *Wash. J.L. Tech. & Arts* 10, (2015): 10 and Michael W. Meredith and Kevin V. Tu, "Rethinking Virtual Currency Regulation in the Bitcoin Age", *Wash. L. Rev.* 90 (2015): 271.

[6] As to Liberty Reserve, this requirement was said to add another layer to the anonymity of the system, according to U.S. government. Ibid.

[7] U.S. Government Accountability Office, GAO-13-516, Virtual Economies And Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks 3 (2013): this source is mentioned in Lawrence Trautman, "Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?", *Rich. J.L. & Tech*. 20, (2014): 13. See also: Joni Larson, "Bitcoin: Same Song, Second Verse, a Little Bit Louder and Little Bit Worse", *MI Tax L.* 41, (2015): 34.

to convert their Linden Dollars into real US Dollars, and subsequently, into any other fiat currency.

There have also been failed attempts to launch virtual currencies; a notable example involved Facebook and its Facebook Credits which were abandoned in less than two years.[8]

Furthermore, the category of potential alternative monies includes also "physical gold and silver coins, and banknotes redeemable into them" and "electronically transferable gold account balances", whose most famous examples are respectively represented by the Liberty Dollar project and E-gold.[9]

The former may be regarded as a controversial example of "community currency".[10] Going into details, the Liberty Dollar was founded by Bernard von Nothaus and his non-for-profit organization NORFED. In the early 2000s, the NORFED "launched its one-ounce silver Liberty piece",[11] whose face value was equal to 10 Dollars and was later raised to 20 Dollars for newly minted coins. In addition, the project offered also dollar-denominated paper certificates that could be converted "at the same par rates for silver kept in storage".[12] Thereafter, the organization introduced also platinum, gold and copper pieces. The ultimate aim of the Liberty Dollar Project was to offer an alternative circulating currency. Notwithstanding such purpose, at first the US Treasury Department confirmed the lawfulness of the project, explaining that Liberty Dollars were neither legal tender nor counterfeit money; nonetheless, in 2006, the US Mint[13] officially stated in a press release that Liberty Dollars "medallions"

[8] Notwithstanding those failures, other business entities have decided to have a try at developing their virtual currency, among which, for instance, Amazon. Hughes and Middlebrook, Regulating Cryptocurrencies In The United States, 813 ff.; Jerry Brito, Andrea Castillo and Houman Shadab, "Bitcoin Financial Regulation: Securities, Derivatives, Prediction markets, and Gambling", *Colum. Sci.* & *Tech. L. Rev.* 16, (2014): 144.

[9] Lawrence H. White, "The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-gold", George Mason University, Department of Economics, Working Paper No 06 (2014): p. 5 ff.

[10] Nikolei M. Kaplanov, "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation", *Loy. Consumer L. Rev*. 25, (2012): 111, 116.

[11] White, "The Troubling Suppression of Competition from Alternative Monies", p. 3 ff.

[12] Ibid. Those certificates amounted to 1, 5 or 10 Dollars.

[13] Cf. United States Mint, "Liberty Dollars Not Legal Tender, United States Mint Warns Consumers", (14 Sept. 2006), *available at* http://www.usmint.gov/pressroom/?action=press_release&id=710&pf.

were designed to compete with US circulating coinage, and, therefore, were in violation of 18 USC § 486 on *Uttering coins of gold, silver or other metal*. Additionally, the press release warned against the fact that such coins might look like official currency due to their inscriptions and images. In 2007, the FBI seized the assets of the Liberty Dollar organization, including gold, platinum and silver, took the computers and files and froze the organization's bank accounts. In 2009, Von Nothaus was charged with violating both 18 USC § 486 and 18 USC § 485, on *anti-counterfeit*. The US government, however, took action against the users of Liberty Dollars as well, declaring that such money could be subject to seizure as contraband.[14]

On the other hand, E-gold Ltd. was a for-profit service, launched in 1996 by Mr. Douglas Jackson and offering "transferable gold-denominated accounts".[15] Jackson claimed that the product was a private currency which was immune from the inflation, unlike traditional fiat currency. E-gold was designed for internet transactions only, and the balance of each account was backed with gold bars that were stored in a warehouse in London. The functioning of E-gold system was rather simple: customers opened their accounts on the E-gold website, then by means of a credit card or a wire transfer they purchased units of gold which could be transferred to other E-gold accounts, and the recipients could redeem such units into fiat currencies. Moreover, customers could virtually carry out all these operations anonymously, in other words under fake names, for no authority checked the registration data.

The E-gold system was at first successful thanks to a number of benefits: (i) it was less expensive than traditional fund transfer systems, (ii) more convenient (especially for migrants in case of remittances),[16] (iii) it offered irreversible transactions, and (iv) its accounts represented a "store

[14] Paul Gilkes, "Liberty Dollars may be subject to seizure", *Coin World* (12 September 2011), *available at* http://www.coinworld.com/articles/liberty-dollars-may-be-subject-to-seizure.

[15] White, "The Troubling Suppression of Competition from Alternative Monies", p. 3 ff.

[16] Remittances have been largely affected by the various legal changes brought forth by electronic payments and financial services. For an analysis of how the U.S. Consumer Financial Protection Bureau (CFPB) has adjusted the cross-border remittance transfer rule in light of the aforementioned changes, see: Hughes and Middlebrook, "Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services", 263 ff.

of value free from political risk".[17] Nonetheless, in December 2005, FBI and the Secret Service Agents raided E-gold locations in Florida, after they discovered that some credit card scammers were using E-gold accounts to transfer unlawfully obtained funds. The Department of Justice found out that the corporation did not comply with the requirements set by the federal regulation in relation to money-transmitting services (FinCEN guidelines),[18] nor did it abide by provisions of the Bank Secrecy Act. As predicated by its founder, E-gold was neither a money transmitter, nor a bank, since it merely transferred the ownership of gold units electronically via the internet, rather than transmitting money, such as for example Western Union, and it did not make loans. In the end, however, Mr. Jackson was sentenced to a period of supervised release, had to turn over more than one million to the government, all E-gold accounts were frozen and E-gold was definitively closed down.

US authorities' measures against Liberty Dollars and E-gold clearly exemplify how much states are troubled by the impact of virtual currencies on both economy and society. Let us therefore sum up the various attitudes displayed by the different countries in relation to the Bitcoin phenomenon.

National Regulatory Attempts and Reactions

Given the transnational and decentralized nature of Bitcoin, concerns about its regulation have been expressed also on both supranational and domestic levels, but thus far no concrete regulatory measures has been taken by international organizations.[19]

---

[17] As claimed by E-gold founder, in White, "The Troubling Suppression of Competition from Alternative Monies", 12 ff.

[18] For an overview of FinCEN regulations, see *infra*, the paragraph titled USA.

[19] In December 2013, the European Bank Authority stepped into the debate on Bitcoins, issuing a formal 'Warning to consumers on digital currencies'. (cf. http://www.eba.europa.eu/documents/10180/15971/EBA+Warning+on+Virtual+Currencies.pdf 2013). Such document aimed at informing investors of the risks connected to the use of virtual currencies, above all, in relation to the 'volatility' of such currencies and the potential thefts, warning also about the fact that if providers of such services were found to be involved in illicit activities, the judicial authority may release a seizure warrant concerning all assets, including those of law-abiding customers. Cf. Cesare Maioli

Anyway, on the domestic level, states have so far adopted fragmented and heterogeneous approaches, and some countries have even displayed different—and at times conflicting—views about Bitcoin-related matters. For the time being, no uniformity can be achieved due to the fact that the phenomenon is still too recent and there is insufficient legal and little economic literature about it; furthermore, there are a number of different interests surrounding the Bitcoin system and those of states themselves which are hard to harmonize.

Nonetheless, some governments have actually taken action in that regard, even though, generally, Bitcoins are struggling to receive regulatory approval, for most countries appear to be rather unsupportive.[20]

An exception to such a common trend is represented by Brazil: in October 2013, the country enacted a statute on the creation and exchange of electronic currencies[21] enabling the Brazilian government to regulate Bitcoins—as well as any other digital currency—by subjecting them to the same rules governing conventional currency. It is noteworthy that pursuant to the terms of the Act, Bitcoins are classified as currency.[22]

As opposed to Brazil, the majority of nations have embraced a more intransigent stand.

The Russian government formally outlawed Bitcoins in February 2014, arguing that such digital currency could enmesh Russian citizens in illicit activities, like money laundering or financing international terrorism.[23]

---

and Maria Letizia Perugini, "Bitcoin tra Moneta Virtuale e Commodity Finanziaria", 17 November 2014: 7 ff. *available at* SSRN: http://ssrn.com/abstract=2526207. In general, however, the position of the EU in relation to Bitcoins is far from clear. So, the EU has not taken any specific position as to the legal status of Bitcoins and Member Countries are left free to decide whether or not to regulate such matter and how to govern it. For instance, the Danish government has declared that the gains or losses generated from casual Bitcoin transactions are exempt from taxation.

[20] According to the website *bitlegal.io*, most of the countries in Europe, along with the USA, Canada, Australia, Argentina and Brazil, and some Asian countries display a 'permissive' approach to Bitcoins, which however in most cases means that no official guidelines or regulations have been passed yet. Whereas, Russia, China, India, Thailand, Jordan and Mexico are defined as 'contentious'. No data are available concerning many African and South America states. Cf. http://bitlegal.io/(last visited September 2015).

[21] Lei n° 12.865, of 9 October 2013; Article 6-VI.

[22] De Filippi, "Bitcoin: A Regulatory Nightmare To A Libertarian Dream", 2 ff.

[23] Maioli and Perugini, "Bitcoin tra Moneta Virtuale e Commodity Finanziaria", 7 ff.

Similarly, Iceland and Vietnam[24] have prohibited their citizens from engaging in foreign exchange trades involving Bitcoins.

However, there are countries which have initially displayed hostility towards Bitcoins but whose current position remains rather controversial.

In Thailand, for instance, the state central banking authority first outlawed the trading of Bitcoins,[25] but, subsequently, softened its position, declaring that Bitcoins could be lawfully traded, provided that they were not converted in or from the national currency.[26]

In the same vein, the Chinese government has shifted from prohibition to mild acceptance and to prohibition back again in a very short period of time. In 2009, following the large spread of QQ (the virtual currency created by Tencen website), China outlawed the use of all virtual currencies. In November 2013, however, the People's Bank of China issued a press release, whereby the institution allowed Chinese citizens to use Bitcoins, even though the government of China confirm it did not intend to recognize Bitcoins as a currency any time soon.[27]

This change of policy was enthusiastically welcomed by Baidu (the Chinese version of Google), and other websites linked to it, which announced that they would start accepting payments in Bitcoins.

Nonetheless, this "opening" lasted less than one month, for in December 2013, the People's Bank of China in a joint statement with four of the major Chinese regulatory organizations[28] formally forbade local banks to accept Bitcoins as currency and financial actors to use them in their transactions.[29] Additionally, in March 2014, the ban was

[24] Apparently, Vietnamese citizens may own Bitcoins, since the ban on the ownership of the cryptocurrency applies to financial institutions only (cf. http://bitlegal.io/ (last visited December 2014).

[25] Matt Clinch, *Bitcoin Banned in Thailand*, CNBC (30 July 2013, 6:20 AM), http://www.cnbc.com/id/100923551: for further information see: Paul H. Farmer Jr., "Speculative Tech: The Bitcoin Legal Quagmire & the Need for Legal Innovation", *J. Bus. & Tech. L.* 9, (2014): 85. *Available at* http://digitalcommons.law.umaryland.edu/jbtl/vol9/iss1/6.

[26] De Filippi, "Bitcoin: A Regulatory Nightmare To A Libertarian Dream", 2 ff.

[27] Farmer Jr., "Speculative Tech: The Bitcoin Legal", 85 ff.

[28] Namely, the China Banking Regulatory Commission, China Securities Regulatory Commission, Ministry of Industry and Information Technology, and the China Insurance Regulatory Commission. See: White, "The Troubling Suppression of Competition from Alternative Monies", 2 ff.

[29] Maioli and Perugini, "Bitcoin tra Moneta Virtuale e Commodity Finanziaria", 7 ff. According to *Bitlegal.io*, China restricts business uses of Bitcoins but permits individuals to own and use Bitcoins in commercial transactions 'at their own risk'. (PBOC Bank Notice No. 239, 2013. Cf. http://bitlegal.io/nation/CN.php.

extended also to payment services, so as to prevent them from transacting with anyone involved in the Bitcoin economy,[30] while, in April 2014, Bitcoin dealers were formally directed to withdraw the amount of money deposited on their accounts because within 15 calendar days such accounts would be frozen.[31]

Alongside the states which have actually taken measures, there are also countries which have thus far preferred to adopt a "wait-and-see" attitude before engaging in determining the legal status of Bitcoins, such as, Italy. Specifically, under Italian law, it may even be superfluous to regulate Bitcoins, since transactions involving them may be regarded as a form of *datio in solutum* in accordance with the principle establishing that everything which is not forbidden is permitted in the end.

Further, there are countries which have opted for a more theoretical approach, and have therefore sought to classify Bitcoins.

In particular, states like Singapore,[32] Finland,[33] Malaysia and Germany permit the purchase, sale and exchange of Bitcoins because, under their domestic laws, Bitcoin is not considered legal tender, but rather a medium of exchange or a commodity.[34] In particular, the German Federal Ministry of Finance has classified Bitcoin as "a financial instrument operating as private money", by employing the expression *Rechnungseinheit*, whose meaning is "unit of account", and which, therefore, excludes Bitcoins from the category of "electronic money". It is noteworthy that the German categorization enables the government to "tax Bitcoin trading as

[30] Notwithstanding the ban, according to the figures of Bitcoincharts.com, BTC China ranks 1st among Bitcoin global service providers with a volume of 4,189,570.452 Bitcoins (cf. http://bitcoincharts.com/markets/ visited on 23 December 2014, whereas U.S. Bitcoin exchanges amount to roughly one-fourth of the Chinese share).

[31] Cf. http://www.techinasia.com/china-banks-must-close*bitcoin*-trading-bank1-accounts/ 2014. See: Maioli and Perugini, "Bitcoin tra Moneta Virtuale e Commodity Finanziaria", 9 ff.

[32] In Singapore citizens are allowed to own, buy, transact and mine Bitcoins, which are however not regarded as a currency, but as a 'taxable service'. Cf. http://bitlegal.io/nation/SG.php.

[33] Finland has recently defined Bitcoins as a VAT-exempt financial service (Ruling of the Finnish Central Board of Taxes, n. 034/2014, of November 2014). Cf. http://bitlegal.io/nation/FI.php. Kati Pohjanpalo, *Bitcoin Judged Commodity in Finland After Failing Money Test*, Bloomberg.com (20 January 2014, 4:50 AM), http://www.bloomberg.com/news/articles/2014-01-19/bitcoin-becomes-commodity-in-finland-after-failing-currency-test.

[34] De Filippi, "Bitcoin: A Regulatory Nightmare To A Libertarian Dream", 2 ff.

short-term capital gains, which opens up the possibility of instituting a sales tax on its use as a means of exchange".[35]

Under the Australian Currency Act 2001, instead, Bitcoins would fall under the category of financial products. Specifically, financial products include non-cash payment facilities, investment facilities and deposit products. A "facility" is broadly defined as, among other things, an intangible property, and Bitcoins are a form of intangible property for they involve the circulation of valuable rights (though not rights to cash as such) which, in turn, belong to the class of intangible property. Moreover, under the aforementioned Act, "a person makes non-cash payments if they make payments, or cause payments to be made, otherwise than by the physical delivery of Australian or foreign currency in the form of notes and/or coins".[36] It follows that Bitcoins are a facility through which individuals can make non-cash payments, and, as such, they amount to financial products under Australian law.[37]

Nonetheless, in 2014, there have been two main developments relating to the legal status of Bitcoins under Australian law.

First, the Australian Taxation Office (ATO) has issued guidelines as to the tax treatment for transactions involving cryptocurrencies, and specifically Bitcoins, stating that the latter are neither currency nor money, but rather their use looks more like barter arrangements.[38]

Secondly, in December 2014, the Australian Securities and Investments Commission (ASIC) has submitted to the Australian Senate an inquiry into digital currency, whereby the commission affirms that digital currencies, such as Bitcoins, "do not fit within the current legal definitions of

[35] Darshan S. Vaishampayan, *Bitcoins are Private Money in Germany*, Wall St. J., The Tell (blog), *available at* http://blogs.marketwatch.com/thetell/2013/08/19/bitcoins-are-private-money-in-germany/. More details in: Paul H. Farmer Jr., *supra* note 27. E. D. Jeans, "Funny Money or the Fall of Fiat: Bitcoin and the Forward-Facing Virtual Currency Regulation", *J. on Telecomm.* & *High Tech. L.* 13, (2015): 99.

[36] Cf. Australian Currency Act 2001.

[37] Rhys Bollen, "The Legal Status Of Online Currencies, Are Bitcoins The Future?", *J. Banking* & *Fin. L.* & *Prac.* (2013): 1–38.

[38] Cf. https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia—specifically-bitcoin/.

a 'financial product'".[39] However, for the time being, both ASIC's document and ATO's guidelines are considered only temporary measures, until the government of Australia officially clarifies the issue.

The above-mentioned examples of national reactions to Bitcoins show that there is still a great deal to be done because, presently, the international landscape is dominated by the uncertainty about the measures to be taken and by non-homogeneous solutions.

At this point, we can turn to the USA, so as to investigate the potential of US proposals as regards Bitcoins, and, in this way, to offer a concrete blueprint as well as a theoretical approach to the phenomenon itself to other legal systems worldwide.

The USA

In light of the initial effects of the phenomenon of cryptocurrencies, the US legislator has immediately engaged in addressing the issues arising from it.

Following the first court decisions (which are going to be debated hereunder), and specifically, since 2013, laws governing Bitcoin transactions have become more stringent: in short, businesses engaging in such operations are required to meet strict reporting and record-keeping standards, implement anti-money laundering programs and comply with the applicable tax regime.[40]

In more detail, the most important step taken by the US government in its commitment to regulate digital currency transactions is represented by the activity of FinCEN in enforcing the Bank Secrecy Act.

In early 2013, the Financial Crimes Enforcement Network (FinCEN), an Agency of the US Department of the Treasury tasked with enforcing

[39] ASIC's Senate Inquiry is available at http://bitlegal.net/nation/AU.php. Anita Ramasastry, *Bitcoin*: *If You Can't Ban It*, *Should You Regulate It*? The Merits of Legalization, Justia.com (25 February 2014), http://verdict.justia.com/2014/02/25/bitcoin-cant-ban-regulate#sthash.4oUpDzhi.dpuf.

[40] Matthew Kien-Meng Ly, "Coining Bitcoin's "Legal-Bits": Examining The Regulatory Framework For Bitcoin And Virtual Currencies", 27 *Harv. J. Law* & *Tec* 27, no. 2, (2014): 587 ff.

the Act, issued guidance[41] on the applicability of the regulations to virtual currencies.[42] The goal of such guidelines was to clearly delineate which activities would make an entity a money services business (MSB), for the purposes of the Bank Secrecy Act, and consequently subject it to FinCEN's registration, reporting, and record-keeping regulations for MSBs. Since then, both federal and state authorities have been constantly supervising Bitcoin activities, although no specific mention of Bitcoin is included in the document. FinCEN guidelines, rather than clarifying the application of the FinCEN regulations on virtual currencies concerning the Bank Secrecy Act provisions falling under the former's scope, have added confusion about it. Specifically, the definitions of "users", "administrators" and "exchangers" included therein are not so accurate and at times the same individual may be qualified as both a user and an exchanger, though according to the applied definition, different legal consequences emerge (for example, users are excluded from the scope of financial regulations on MSBs).[43] Nevertheless, Bitcoins may be classed as a decentralized virtual currency (DVC) pursuant to the categorization requirements set out in the guidance document, since DVCs are defined as currencies having "no central repository and no single administrator", and "persons may obtain [their units] by their own computing or manufacturing effort".[44]

The actual application of FinCEN guidelines to Bitcoins would result in two major implications for the cryptocurrency itself and its users.

First, a user selling Bitcoins,[45] whether as an individual or as a business, would be considered a money transmitter and would therefore be subject to FinCEN's regulations for MSBs. Specifically, an individual who mines Bitcoins and exchanges them for other goods or services is not identified as a money transmitter. Whereas, an individual who mines Bitcoins and exchanges them for real currencies, or an individual who serves as an

[41] The FinCEN guidance document "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." For an overview of the guidance on virtual currencies issued by the FinCEN, see Sarah Jane Hughes and Stephen T. Middlebrook, *supra* note 16.

[42] Kien-Meng Ly, "Coining Bitcoin's "Legal-Bits", 587 ff.

[43] Cf. Joshua Fairfield, "*Bitproperty*", in 88 *S. Cal. L. Rev.* (2015): 805 ff.

[44] Kien-Meng Ly, "Coining Bitcoin's "Legal-Bits", 587 ff.

[45] Farmer Jr., "Speculative Tech: The Bitcoin Legal", 85 ff.

intermediary to such a transaction, is each labelled as a money transmitter.[46] It follows that any individual or entity which is labelled as "money transmitter" has to register with the Secretary of the Treasury as a MSB, for if they do not, they may face civil or criminal liability.

Second, it appears as though any business facilitating the conversion between Bitcoin and US Dollar would be considered an "exchanger" according to the guidance document and would thus be subject to FinCEN's regulations for MSBs. It might be argued, therefore, that the ultimate objective pursued by FinCEN regulation is to neutralize the most part of anonymity benefits connected to the use of Bitcoin.[47]

Furthermore, it is worth noticing that along with the Bank Secrecy Act and the FinCEN regulation, the US government has taken another measure in response to the spread of Bitcoins among American users, that is the IRS's guidance,[48] on the basis of which Bitcoin will be treated as "property" for federal tax purposes.[49]

Together with the US federal legislation, also state legislators have engaged in developing their own solutions in relation to Bitcoins, which are mostly in line with the principles set out in federal laws, such as tax regulations and the FinCEN guidelines.

For instance, in July 2014, the Department of Financial Services of the State of New York has proposed a regulation draft, named *BitLicense*, "relating to the conduct of business involving Virtual Currency", defined as "any type of digital unit that is used as a medium of exchange or a form of digitally stored value or that is incorporated into payment system technology", but broadly construed so as "to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort".[50]

---

[46] Ibid.

[47] Kien-Meng Ly, "Coining Bitcoin's "Legal-Bits", 587 ff.

[48] Internal Revenue Service (IRS) Notice of 31 March 2014.

[49] Ibid.

[50] http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf.

This definition excludes online game currencies and digital units that are exclusively used as "part of a customer affinity or rewards program",[51] however it seems to encompass Bitcoins.

US Courts' Classificatory Attempts

According to the definition of the inventors of Bitcoins, they are a peer-to-peer electronic cash system.[52]

Even though Bitcoin's developers apparently want Bitcoin to become a new type of money—such intention is also mirrored in the very name of the cryptocurrency which contains the word "coin"—US courts have neither unanimously nor uncritically embraced such classification.

In truth, two main categorizations emerge from court decisions, namely, the definition of Bitcoins as either a currency[53] or a commodity.

The "classification" of Bitcoins as "currency" is supported by a case which started in 2013, when the Securities and Exchange Commission (SEC) filed a complaint against Trendon T. Shavers and the Bitcoin Savings and Trust (BTCST) in the US District Court for the Eastern District of Texas, Sherman Division (case *SEC* v. *Shavers*[54]). This was "the first SEC enforcement action involving Bitcoins"[55] and it showed the dangers of the application of the Ponzi Schemes to Bitcoin investments. In short, according to SEC, Shavers offered and sold fraudulent investments in BTCST, which was a "Bitcoin-denominated Ponzi Scheme founded and operated by [him]",[56] over the internet. By promising up to 7 % returns on a weekly basis thanks to its alleged trading of Bitcoins against

[51] Ibid.

[52] Satoshi Nakamoto, *Bitcoin*: *A Peer-to-Peer*.

[53] Casey Doherty, "Bitcoin and Bankruptcy—Understanding the Newest Potential Commodity", in 33–7 *ABIJ* 38, 2014.

[54] *Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust*, Civil Action No. Civil Action No. 4:13-CV-416. The complaint filed by SEC which started the court litigation action against Shavers is available at https://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf.

[55] Daniel Gwen and David E. Kronenberg, "Bitcoins in Bankruptcy: Trouble Ahead for Investors and Bankruptcy Professionals?", *Pratt's Journal of Bankruptcy Law*, February/March (2014): 112–121.

[56] Cf. https://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf.

US Dollars, Shavers managed to obtain more than 700,000 Bitcoins in just 1 year (from September 2011 to September 2012). By reason of the foregoing, SEC claimed that Shavers and BTCST were in violation of the Security Act and the Exchange Act and requested, therefore, that the court pass an order "[p]ermanently restraining and enjoining Defendants, […] from violating Sections 5 and 17(a) of the Securities Act [15 USC §§ 77e and 77q(a)], and Section 10(b) of the Exchange Act [15 USC § 78j(b)] and Rule 10b-5 thereunder [17 CFR § 240.10b-5]; […] [and] [o]rdering Defendants to disgorge their ill-gotten gains received as a result of their violations of the federal securities laws".[57] The court entered final judgment on 18 September 2014, and found that Shavers and BTCST violated the aforementioned statutes and required them to pay more than USD40 million in disgorgement and prejudgment interest, coupled with a civil penalty of USD150,000 each.[58]

This case is noteworthy because the District Court determined that Bitcoins "can be used as money",[59] and, in so doing, it upheld the definition of Bitcoin as "a virtual currency that may be traded on online exchanges for conventional currencies, including the US Dollar, or used to purchase goods and services online"[60] (as set forth in the complaint filed by SEC to the court) subjecting it to US banking law.[61]

Nevertheless, since such a case dealt with an in-kind "Bitcoin-for-Bitcoin" exchange and the SEC is concerned with exchanges of commodities for money (Dollars), the definition given by the court could not be broadly applied beyond the case facts. It is worth adding, though, that Bitcoins were defined as currency for SEC jurisdiction purposes, since, although the court decision represents a merely persuasive precedent, in my opinion, in case of future similar cases the SEC may nonetheless use the same argument to obtain jurisdiction. Furthermore, if Bitcoins were defined as currency pursuant to the Bankruptcy Code, contracts whereby individuals exchange Bitcoins for real currencies would amount

[57] Ibid.

[58] Cf. http://www.sec.gov/litigation/litreleases/2014/lr23090.htm.

[59] Gwen and Kronenberg, "Bitcoins in Bankruptcy", 112 ff.

[60] Cf. https://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf.

[61] Gwen and Kronenberg, "Bitcoins in Bankruptcy", 112 ff.

to "swaps" under §§ 362 and 546 of said Code, and swaps are granted great protection against bankruptcy. In other words, applying the definition of currency to Bitcoins under the Bankruptcy Code would result in treating any entity that cashes in Bitcoin for Dollars the same as an entity that swaps Swiss Francs for Dollars.[62]

Whereas, the qualification of Bitcoins as a commodity stems from the case *In re CLI Holdings*,[63] whereby the court treated Bitcoins like a "subterranean commodity" (for example oil), due to the similarities arising from the "extraction process" shared by both of them.

The case at issue involved, on the one hand, CLI Holdings Inc., that is the debtor, and, on the other hand, Bitvestment Partners LLC, the creditor. The debtor was a corporation doing business under the "Alydian" trade name, whose main shareholder was CoinLab Inc., and which engaged in operations of mining Bitcoins.[64] But, the creditor was a Bitcoin-financing entity, which engaged in Bitcoin-related business and opportunities.[65]

In August 2013, Bitvestment entered into an Amended and Restated Bitcoin Services Agreement (hereinafter, Amended Agreement) with CoinLab and CLI Holdings Inc. Under the terms of the Amended Agreement, Bitvestment paid $75,000 to the debtor and CoinLab, while the latter, pursuant to the contractual requirements, would have had to use their "best efforts" and "dedicate 100 % of [their] mining output" to producing Bitcoins for Bitvestment until Bitvestment would have received the agreed-upon amount of 7,984.006735 Bitcoins. Hence, the creditor financed the former's venture in exchange for a defined amount of Bitcoins produced. In short, "Bitvestment received a virtual overriding

[62] Casey Doherty, "Bitcoin and Bankruptcy". A swap is a contract in which each counterparty agrees to an exchange of payments related to the value or return of some underlying asset or event. The structure of Bitcoin swaps may resemble a foreign exchange (FX) swap. In an FX swap, two parties borrow a foreign currency from each other and agree to pay each other back at a specified exchange rate.

[63] *In re CLI Holdings*, Case No. 13–19,746 (W.D. Wash. 2013).

[64] Specifically, in exchange for a yearly fee, CLI Holdings 'would set up, maintain, and operate the hardware necessary to mine Bitcoin for large institutional investors, with any Bitcoins mined belonging to the investors' (Gwen and Kronenberg, "Bitcoins in Bankruptcy", 112 ff).

[65] All documents concerning the case I*n Re CLI Holdings Inc.* are available at http://www.plainsite.org/dockets/unc1p5dn/washington-western-bankruptcy-court/cli-holdings-inc/.

royalty interest (ORRI)"[66]—which is popular in the oil and gas industry—on the production of Bitcoins.

However, since the value of Bitcoins was peaking at the time, the debtor started to be overwhelmed by oppressive ORRIs and, as a consequence, the debtor and CoinLab breached the Amended Agreement by failing to deliver the Bitcoins mined.

As a result, on 29 October 2013, Bitvestment filed a lawsuit in the US District Court for the Southern District of New York against the debtor, seeking, among other things, specific performance for defendants to mine and deliver 7,984 Bitcoins to Bitvestment. The case brought before the court was rather similar to bankruptcy cases involving oil and gas industry companies producing for the first time in states where no ad hoc laws had been developed to regulate such issues.

On 5 November 2013, the District Court stayed the action against the debtor because on 1 November 2013, Alydian filed a voluntary Chap. 11 case; consequently, the court entered a Temporary Restraining Order to compel CoinLab to begin mining and delivering the contracted-for Bitcoins to Bitvestment, pursuant to the terms of the Amended Agreement.

Thereafter, on 15 November 2013, the debtor filed a motion to reject Executory Contracts, in which it was argued that "it should be allowed to reject the Amended Agreement pursuant to 11 USC § 365 because it is an 'executory contract' within the meaning of 11 USC § 365".[67] The debtor wanted to reject the contract concluded with Bitvestment, so as to be free to sell its production on the market, but the creditor argued that such a contract could not be rejected. The court, by relying on precedents in the oil and gas industry, held that Bitvestment was right and the debtor could not reject the contract, since an agreement "where the only performance of the interest-holder was to receive production" could not be subject to rejection.[68]

[66] Casey Doherty, "Bitcoin and Bankruptcy".

[67] Cf. Motion to Reject Executory Contracts, cf. http://www.plainsite.org/dockets/unc1p5dn/washington-western-bankruptcy-court/cli-holdings-inc/.

[68] Casey Doherty, "Bitcoin and Bankruptcy".

At this point, the debtor, being unable to perform its obligations associated with each of the Bitcoin Services Agreements it had concluded, including the one with Bitvestment, resolved that it could not generate a positive cash flow from the mining operation, therefore, it requested the court to enter an order "approving bidding procedures for a sale under 11 USC § 363 *et seq.* and BR 9013, and setting a hearing on sale of assets"[69]; in other words, it tried to sell its mining rigs. However, Bitvestment questioned the actual necessity of such a rushed sale in light of the fact that "the rigs were producing a healthy amount of valuable Bitcoin post-petition". Since the production was "rich" and no better evidence was produced before the court, the latter did not approve the debtor's rushed sale. In the end, by preserving Bitvestment's rights, the two parties "settled their dispute confidentially and the case was dismissed".[70]

This case exemplifies the murkiness currently affecting the legal status of Bitcoins.[71] As a matter of fact, Bitvestment did not have a lien on the debtor's rigs to mine Bitcoins. In the oil and gas industry, the ultimate worth lies with the well or mine themselves, where the minerals are to be found, even though the rigs are of great value. Whereas, in case of Bitcoins, the rigs represent the most valuable asset, for Bitcoins may—and actually are—produced anywhere, but what matters is the CPU power you supply to the net.[72]

Moreover, according to us, the parallel between Bitcoins and the oil and gas industry precedents was due to three concomitant factors: (i) the agreement concluded between CLI Holdings Inc. and Bitvestement (that is, Amended and Restated Services Agreement) is a type of contract which is commonly employed in the oil and gas industry; (ii) the terminology used in the oil and gas industry is in part mirrored in the Bitcoin domain; (iii) the background of the case at issue shares many

[69] Cf. *Motion For Order Approving Notice Of Sale, Bidding Procedures Order, And Setting Hearing On Sale Of Assets And Granting Other Relief*, available at http://www.plainsite.org/dockets/unc1p5dn/washington-western-bankruptcy-court/cli-holdings-inc/.

[70] Casey Doherty, "Bitcoin and Bankruptcy".

[71] The author affirms that Bitcoin-holders face confusion over how they can perfect their interest, that is, as a commodity, as a security or as simple cash. Ibid.

[72] Since Bitvestment had no lien on the rigs, if the court had approved their sale, the former would have been left quite vulnerable.

elements with the facts of other legal precedents concerning supply contracts within the oil industry.

Anyhow, it might be argued that, although the parallel drawn between Bitcoins and subterranean commodities—especially oil—is conditional, fortuitous and expressed only in *obiter dicta*, it has nonetheless granted US legal interpreters the chance to draw on the wide repertoire of mining law.

US Potential Regulatory Frameworks for Bitcoins

The trend towards adaptation which encourages the inclusion of new circumstances into pre-existing patterns is typical of the common law legal theory, and that of the USA in particular, and it is not restricted to the activity of the courts, as described above.

In this regard, according to the options proposed by the legal theory, the regulation of Bitcoins and digital currencies under the US legal system may fall under one of the following existing legal frameworks, namely: (i) the Bank Secrecy Act, (ii) Securities Regulations, (iii) the Stamp Payments Act, (iv) the Electronic Fund Transfer Act, (v) the RICO (Racketeer Influenced and Corrupt Organizations) Act, and (vi) the Uniform Commercial Code.[73]

(i) The **Bank Secrecy Act** (BSA)[74] was enacted in order to prevent money laundering on the part of financial institutions, which are defined, for the purpose of the Act, as MSBs and have to comply with specific requirements, among which the need to "register with the government, implement anti-money laundering procedures",[75] and keep records of their activities. In addition, MSBs must report cash transactions exceeding $10,000 as well as any suspicious activ-

[73] Kien-Meng Ly, "Coining Bitcoin's "Legal-Bits", 588 ff. A similar attempt to identify the applicable source of law/regulation under U.S. legal system is carried out by Nikolei M. Kaplanov: Kaplanov, "Nerdy Money, 11 ff.

[74] This regulation was codified in Title 31 of the Code of Federal Regulations Chapter X, the Currency and Foreign Transactions Reporting Act of 1970.

[75] *FinCEN's Mandate from Congress*, Dep't Of The Treasury Fin. Crimes Enforcement Network, http://www.fincen.gov/statutes_regs/bsa.

ity, ranging from money laundering to tax evasion.[76] The main issue arising in relation to the application of BSA to Bitcoins is whether or not the latter should actually be labelled "currency" for the purposes of the Act, even though no conclusive definitions are included therein.[77] Anyhow, if BSA was actually applied to the Bitcoin system, this would impose great restrictions on it, although such requirements have been established in order to improve the security and lawfulness of MSBs. Specifically, any exchange of digital currency for a traditional currency would fall under the scope of the Act and, therefore, any business entity that carries out such transactions would be required to register with the government, implement the relevant anti-money laundering measures and consequently lose the advantage of anonymity.

(ii) The second proposal concerns the securities regulations set forth in the **Securities Exchange Act of 1934** (SEA) which governs the exchange of securities, encompassing notes, stocks and investment contracts. In order for Bitcoins to be governed by the SEA, they should be considered a form of security, since currencies are excluded from the purview of the Act. The problem is that Bitcoin lacks the distinctive characteristics of the aforementioned categories of securities, namely: (a) it is not used to make a promise about the payment of an amount of money (as opposed to notes)[78]; (b) it is different from a stock, since it does not confer specific rights to its holder[79];

[76] Cf. 31 USC § 5312 et seq., http://www.law.cornell.edu/uscode/text/31/5312.

[77] Cf. 31 USC § 5312 (3) et seq., http://www.law.cornell.edu/uscode/text/31/5312.

[78] A note can be either a negotiable instrument or a security. See Reves, 494 U.S. at 67 (discussing the family resemblance test as it applies to the differentiation between notes). A Bitcoin is not a negotiable instrument because it is not an '*unconditional promise or order to pay a fixed amount of money*'. U.C.C. § 3–104(a) (2013). To determine whether a note is a security the courts apply the family resemblance test on which see Reves, 494 U.S. at 67 and Farmer Jr. argues that applying that very same test a court might also qualify Bitcoins as a security (Farmer Jr., footnote 25, 99–100). Although, in this author's opinion, this is a merely a stratagem to do away with anonymity in this area.

[79] In the case of stocks the Supreme Court has identified main features as '(*i*) *the right to receive dividends contingent upon an apportionment of profits*; (*ii*) *negotiability*; (*iii*) *the ability to be pledged or hypothecated*; (*iv*) *the conferring of voting rights in proportion to the number of shares owned*; *and* (*v*) *the capacity to appreciate in value*.' United Housing Foundation, *Inc.* v. *Forman*, 421 U.S. 837, 851 (1975). Bitcoins**,** although transferable and able to appreciate, do not carry the right to a dividend, the right to vote nor, any other rights at all connected to any legal entity.

and (c) it cannot be regarded as an investment contract because purchasing Bitcoins through a currency does not amount to an investment according to the definition given by the leading cases.[80]

(iii) One of the most recurrent hypotheses concerning Bitcoins' regulation in literature relates to the **Stamp Payments Act** (SPA) of 1862, even though in practice, this solution appears to be rather unfeasible since the SPA forbids the issuance and circulation of any token "for a less sum than $1, intended to circulate as money or to be received or used in lieu of lawful money of the United States".[81] The main aim pursued by said Act "was to protect the value and use of US coins against unofficial competing currencies".[82] In order to gain a better insight on the actual meaning of the SPA, it is necessary to rely on early case law (for no court decision has been published on the matter since 1899). For instance, in the case *United States* v. *Van Auken* (*United States* v. *Van Auken*, 96 US 366 (1877)) the Supreme Court held that the Congress's primary aim in passing such Act was "to prevent competition with the national currency". Therefore, its provisions did "not apply to anything with a limited circulation",[83] neither did they apply to anything which did not mirror the national official currency. Hence, the actual applicability of the SPA to Bitcoins depends on whether the latter may be regarded as a

[80] Investment contracts have been defined as 'contract[s], transaction[s], or scheme[s] whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party.' *SEC* v. *W.J. Howey Co.*, 328 U.S. 293, 298–99 (1946). To determine whether a contract qualifies as an investment contract, courts apply the three pronged Howey test requiring proof of (i) an investment of money, (ii) a common enterprise, and (iii) the expectation of profits to be derived from the efforts of others. And Bitcoins fail two of these three prongs. First, Bitcoin purchasers who buy Bitcoins anticipating profits do not expect these profits to result from the actions of a promoter but on market forces. In addition to that, the protocol does not rely on third parties and each party acting in the Bitcoins system acts wholly in self-interest. This is not to say 'there could be no securities involving Bitcoins; indeed, equity interests in exchanges or other businesses dealing in the periphery of the Bitcoin economy would obviously be securities'. J. Scott Colesanti, "Trotting Out the White Horse: How the S.E.C. can handle Bitcoin's Threat to American Investors", *Syracuse L. Rev.* 65, (2015): 1 ff.; Nicole D. Swartz, "Bursting the Bitcoin Bubble: The Case To Regulate Digital Currency as a Security or Commodity", *Tul. J. Tech.* & *Intell. Prop*. 17, (2014): 319, 329–330.

[81] 18 U.S.C. § 336.

[82] Kien-Meng Ly, "Coining Bitcoin's "Legal-Bits", 587 ff.

[83] *Van Auken*, 96 U.S. at 367–68.

"competing currency". As a matter of fact, Bitcoin's use does not detract from the value of US coins since, first of all, such cryptocurrency has been designed for internet transactions only and as such, at least on a theoretical level, cannot compete with official fiat currencies.[84] Besides, the very enforcement of the provisions of this Act would be problematic, since Bitcoins do not have a central authority that can be prosecuted by the US government.

(iv) A further suggestion takes into account the **Electronic Fund Transfer Act** (EFTA) of 1978 which lays down a "framework establishing the rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems".[85] This Act may seem a viable solution, given the electronic nature of Bitcoins and their transfer via the internet; however, the "participants" referenced in the EFTA are meant to be financial institutions engaging in or facilitating electronic fund transfers. And, since Bitcoins cannot be recognized as a legal entity, neither does an official Bitcoin entity or intermediary exist which may order to transfer funds electronically, and to rely on applying the EFTA regime to Bitcoins does not seem an adequate solution either.[86]

(v) A potential solution to tackle Bitcoins-related criminal activities may involve the **RICO Act**.[87] The Act was passed in 1970, in order to combat organized crime and, in particular, individuals engaging in various illicit activities; to this end, the RICO lays down the criminal penalties[88] for those in violation of any provision of its Section 1962. Such section establishes that "it shall be unlawful for any person who has received any income derived, directly or indirectly, from a pattern of racketeering activity or through collection of an unlawful debt in which such person has participated as a principal […], to use or

[84] According to some legal scholars, Bitcoin cannot fall under the scope of the Stamp Payments Act for it does not possess the above-mentioned 'physical' characteristics that distinguish money (cf. Joshua J. Doguet, *supra* note 2).

[85] 15 U.S.C. § 1693(b) (2012).

[86] Kien-Meng Ly, "Coining Bitcoin's 'Legal-Bits'", 587 ff.

[87] 18 U.S. Code, Ch. 96.

[88] Cf. 18 U.S. Code, § 1963 – *Criminal Penalties*, available at http://www.law.cornell.edu/uscode/text/18/1963.

invest, directly or indirectly, any part of such income, or the proceeds of such income, in acquisition of any interest in, or the establishment or operation of, any enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce."[89] The definition of "racketeering activity" included in the RICO Act encompasses a number of different criminal acts, such as, "murder, kidnapping, gambling, arson, robbery, bribery, extortion",[90] counterfeiting activities, wire frauds, laundering of monetary instruments, activities related to illegal money transmitters, and so on. Hence, in light of this broad definition, it might be suggested that criminal activities accomplished via Bitcoins (for example, money laundering or frauds) may fall under the purview of the RICO and, in so doing, individuals committing them may actually be prosecuted.

(vi) The last potential legal framework may be provided by the **Uniform Commercial Code** (UCC). This Code establishes a number of provisions aimed at regulating sales and other commercial contracts. For the purposes of the UCC, it does not matter which definition is attached to Bitcoins (either currency or commodity), since in both cases transactions involving Bitcoins will be recognized and validated under this Act.[91] This solution would however grant only a general regulatory framework since the UCC governs all sales contracts and in this way it indirectly governs also any sale and purchase of Bitcoins, even though it includes neither an explicit reference to them nor an ad hoc provision in that regard.

Bitcoins: Currency or Commodity? The Legal Theory's Viewpoint

In order to apply the Acts which have been briefly described above, it is necessary, first of all, to understand what Bitcoins really are.

[89] 18 U.S. Code, § 1962 – *Prohibited Activities*, available at http://www.law.cornell.edu/uscode/text/18/1962.

[90] 18 U.S. Code, § 1961 – *Definitions*, http://www.law.cornell.edu/uscode/text/18/1961.

[91] Kien-Meng Ly, "Coining Bitcoin's "Legal-Bits", 587 ff.

According to the "conventional" reconstruction of the history of money, after a period in which people relied on barter only, one of the commodities which was previously used for such purpose emerged spontaneously over the others and assumed the role of a medium of exchange thanks to "its superior saleability and its scarcity, durability and portability".[92] Over the centuries, money, little by little, acquired its current form, mainly thanks to financial institutions and state authorities in its current form: fiat money.

On the basis of this reconstruction, money is regarded as a numeraire, that is, a "nominal signifier of value that does not contain any value itself",[93] but which represents the final outcome of a social convention. Those who advocate in favour of the definition of Bitcoin as money (that is most proponents of Bitcoins) draw a parallel between the aforementioned evolution of money and the creation of Bitcoins. In particular, they argue that Bitcoin has been launched into the market as if it were one among several commodities available to users, and due to its scarcity and ease of circulation, it has gained in value and, consequently, it may evolve into a form of money if the majority of market participants eventually acknowledged its benefits.[94]

The main shortcoming of this argument lies, however, in the fact that people already have a medium of payment and exchange, that is, traditional currencies; hence, Bitcoins could at best amount to an alternative or a competing monetary system.

---

[92] Beat Weber, "Can Bitcoin compete with money?", *Journal of Peer Production* 4 (2014): 1000 ff., *available at* http://peerproduction.net/issues/issue-4-value-and-currency/invited-comments/can-bitcoincompete-with-money/.

[93] Sonal Mittal, *Is Bitcoin Money*? *Bitcoin and Alternate Theories of Money*, Independent Writing Project, (Spring 2013).

According to economics money is traditionally defined as a medium of exchange, a unit of account, and a store of value. Richard W. Rahn, "A Constant Unit of Account", *Cato Journal* 30, no. 3 (2010): 521–522. Its legal definition, however, is far more elusive. For example, Black's Law Dictionary defines money as '[t]he medium of exchange authorized or adopted by a government as part of its currency.' BLACK'S LAW DICTIONARY 695 (9th Ed. 2009). See U.C.C. § 1–201(b)(24) (2013) and 11 C.F.R. § 100.52(c) (2013). The operative clause here is that, in order for something to be deemed money, it has to be described as such by a government.

[94] Ed Howden, "The Crypto-currency Conundrum: Regulating an Uncertain Future", *Emory Int'l L. Rev*. 29, (2015): 741–743.

Nonetheless, the "conventional" understanding of money, as described above, is challenged by an alternative constitutional theory according to which money is a "constitutional project […] with transfer-enabling properties that have a 'real value'".[95]

In fact, owing to the historical and practical circumstances, people could not have spontaneously turned to coins, but rather the latter started to be minted as a form of governance, that is as a way through which the sovereign authorities could carry out their activities.

However, either way, at this point in time, Bitcoins can hardly be considered money, for they constitute "a difficult medium of exchange and a poor unit of account and a store of value".[96]

Furthermore, Bitcoins may only become a competing monetary system if they manage to offer advantages and economic benefits that outweigh those—either existing or perceived by customers—of the conventional system. In other words, switching from the traditional monetary system to the Bitcoin system should be convenient both in terms of cost and prospects and would require a widespread adhesion, since "the benefit of using the network rises with the number of participants".[97] Therefore, Bitcoin has to succeed in overcoming lock-ins in existing currencies in order to stand out as a viable alternative to them.

Besides, another feature which weakens Bitcoins' definition as currency is its high volatility, a characteristic which makes them extremely attractive in the eyes of speculative traders, but not as a unit of account.

Furthermore, since the amount of Bitcoins is limited, individuals who own them are more prone to hoarding rather than spending them in view of an appreciation of their stock in the future, due to the growing demand of this cryptocurrency. Nonetheless, hoarding decreases the amount of circulating Bitcoins, consequently hindering their possibility to become a widespread medium of payment. And, even if hoarding may help Bitcoins develop into a store of value, its high volatility downplays this feature, making them largely speculative. In other words, it might be

[95] Ibid.

[96] Ibid.

[97] Weber, "Can Bitcoin compete with money?", 1000 ff.; Eric P. Pacy, "Tales from the Cryptocurrency: On Bitcoin, Square Pegs, and Round Holes", *New Eng. L. Rev.* 49, (2014): 121, 138.

argued that Bitcoins' architecture itself prevents this cryptocurrency from actually developing into an alternative and competing form of money.[98]

Although attempts may be made to class Bitcoins under other categories (such as, notes, credit instruments, bonds, and so on), in all likelihood, unanimity can hardly be reached; in this case, Bitcoins can be much more easily classified, on a residual basis, as commodities.

As a matter of fact, given the drastic price swings.[99] Bitcoins are commonly considered and treated as a commodity by most of their holders and sellers. Besides, the lack of supervision coupled with the pre-determined maximum amount of Bitcoins may ultimately impact on Bitcoins' supply, which may also be strongly affected from outside events, and all these elements encourage Bitcoins' equation with a commodity.[100]

Moreover, the fact that Bitcoins may be considered a commodity has evident consequences from a financial perspective, for such a categorization enables firms to create Bitcoin derivatives.[101]

Derivatives, as it has been demonstrated also by the recent economic crisis, are rather risky financial instruments, however, it seems that if applied to Bitcoins they might turn out to be economically useful. The development of Bitcoin derivatives serves, in fact, a twofold purpose, that is to help anyone that accepts or holds Bitcoins to decrease the price risk to which they are exposed due to the high price volatility and to "enable parties to invest in Bitcoin without actually holding Bitcoins".[102]

---

[98] Weber, "Can Bitcoin compete with money?", 1000 ff.

[99] According to the website *bitcoinaverage*, on 19 January 2015, the USD average market value of a Bitcoin amounted to USD211,90; on 20 January 2015, the USD average market value of a Bitcoin amounted to USD206,93; on 21 January 2015, the USD average market value of a Bitcoin amounted to USD214,31 and on 22 January 2015, the USD average market value of a Bitcoin amounted to USD232,28 (cf. https://bitcoinaverage.com/#USD).

[100] Furthermore, Bitcoin may fall under the definition of 'commodity' provided for by the U.S. Commodity Exchange Act (CEA). Houman B. Shadab, *Regulating Bitcoin and Block Chain Derivatives*, *Written Statement to the Commodity Futures Trading Commission*, *Global Markets Advisory Committee*, *Digital Currency Introduction – Bitcoin*, 9 October 2014. *Available at SSRN*: http://ssrn.com/abstract=2508707.

[101] Nowadays, several firms have begun offering Bitcoin derivatives: alongside ICBIT which claims to be the first Bitcoin future Market, in September 2014, OKCoin (a Bitcoin exchange located in China) started offering Bitcoin-USD futures, and a Cyprus-based firm (Anyoption) offers Bitcoins binary options. Ibid.

[102] Ibid.

In truth, however, not only are Bitcoins unfit to be considered currency, but at the same time, it might be argued that they rather amount to a specific category of commodity, which may be defined as "synthetic commodity money".[103] The difference between rule-bound fiat money and synthetic commodity money is that "real resource costs alone limit monetary base growth in a synthetic commodity-money regime, whereas in rule-based fiat money regimes […] base growth is limited by positive *transactions* costs, including any penalties to which rule-violating authorities are subject".[104]

In other words, the very existence of fiat money presupposes the presence of a monetary authority which can manage its quantity. In a managed monetary system, there is an instrumental use of the price level or other macroeconomic variables. Whereas, the synthetic commodity money gives rise to an "automatic monetary system" in which "monetary policy as such consists solely of the designation of a single commodity or service as the basis for the monetary unit."[105] Therefore, in such a regime there is no need for a monetary authority (either one tasked with the discretionary management of the money base or the enforcement of monetary rules, as opposed to a managed monetary system). So, the fundamental distinguishing characteristic of the synthetic commodity money "is precisely that by resorting to it one can avoid leaving the management of money *either* to central bankers *or* to the blind forces of nature".[106]

Additionally, since synthetic commodity money can only be used for monetary uses, its purchasing power will not be altered by a non-monetary demand for it.

An example, even though an unplanned one, of a synthetic commodity money was the Iraqi Swiss Dinar.

---

[103] George Selgin, "Synthetic Commodity Money", (April 2013), available at: http://ssrn.com/abstract=2000118.

[104] Ibid.

[105] Ibid.

[106] Ibid. According to Daniela Sonderegger, "A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation", *Wash. U. J.L. & Pol'y* 47, no. 175 (2015): 205 Bitcoin is Inherently Self-Regulating: 'Bitcoin is an open source protocol that can be molded and built upon by its users, thereby exhibiting self-regulating qualities'.

The Iraqi official currency before the Gulf war of 1990 was made up of paper Dinars which were printed in the UK by means of Swiss-engraved plates (called Swiss Dinars). During the war, it was not possible to import such notes, and after the end of the war, Hussein's government decried the previous currency and issued the "Saddam" Dinars in place of it. Nonetheless, Saddam Dinars were issued on such a huge scale—not only by the government but also by counterfeiters—which led to its quick depreciation. In the meantime, Swiss Dinars continued to circulate in the Kurdish regions of the country, holding a rather stable purchasing power as well as an exchange rate relative to US Dollars, regardless of their "physical" deterioration due to their constant use. Over the years the exchange rate between Saddam and Swiss Dinars continued to rise, until 2003 when it reached 300:1. In order to stabilize the Iraqi official currency, the Coalition Provisional Authority pegged the Saddam Dinar to the Swiss Dinar at a rate of 150:1, and, at the same time, it provided for the new production of the official paper notes through the original Swiss plates, modifying however their denominations so as to make them correspond to those of the Saddam Dinars.

So, Swiss Dinars after being officially abandoned as the fiat currency of the Iraqi State, became a synthetic commodity currency: though being devoid of any intrinsic value, it continued functioning as money without the support of the legal-tender status and while being officially condemned.

Similar to the Swiss Dinars, Bitcoin is backed by neither a government nor a genuine commodity, nonetheless, users trust it as Iraqis trusted the old Swiss Dinars, whose value, against all odds, remained stable for over a decade.[107]

Conclusions

The Bitcoin case is a clear example of how the domain of law deals with social and technological innovations: in general, rather than changing their inner patterns, legal systems adapt themselves to unfamiliar circum-

[107] Reuben Grinberg, "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Sci.* & *Tech. L.J.* 4, (2012): 159.

stances, seeking to regulate the new with the old, by relying on traditional legal institutes and tailoring them to the new environment, without formulating ad hoc legislations.

Vis-à-vis Bitcoin's potentially revolutionary consequences, the US legal formants have reacted by searching for a categorization of said phenomenon which would enable the legal interpreter to place Bitcoin in one of the blocks making up the existing classification. And, even though the type of reaction which emerges from their commitment is fragmented and mostly uncoordinated—each legal formant has, in fact, autonomously developed different solutions—their engagement represents in any case an important first step.

Specifically, the legislation has focused on whether or not a concrete regulation of Bitcoin was necessary; presently, however, the most significant proposal in this regard concerns the suggestion to introduce a license system (for example, *BitLicense* proposed by Department of Financial Services of the State of New York). Whereas, the academicians and the courts have preferred to endorse the approach towards the adaptation of law rather than its transformation.

In particular, legal expert has sought to identify under the purview of which Act the concept of Bitcoin could eventually fall. Nonetheless, as it emerged from our analysis, the choice to rely on pre-existing regulatory patterns has proved to be not fully effective. The major practical obstacle of such an approach lies in the "design" of the statutes themselves since they do not include any definition of "Bitcoin". Hence, none of the Acts which have been examined appears suitable for a thorough regulation of Bitcoins, because neither do they contain specific provisions governing Bitcoins nor would they duly address Bitcoins-related issues.

On the other hand, the judiciary has achieved important and promising results by interpreting analogically a chain of legal precedents, and as a result bypass the need to formulate a definition of Bitcoins. This outcome amounts to the true innovation in relation to Bitcoin's potential regulation, for the approaches followed by the other legal formants represent instead typical examples of the *modus operandi* of the legal domain. In short, such a parallel stems from a sort of empathy with mining law court decisions dating back to earlier times and relating to different—though comparable—legal circumstances (or maybe, they might be regarded as

an accident, or a brilliant subterfuge or even the example of the ability of making a virtue out of a necessity).

Thus, philosophically speaking, it is as if the internet had offered a virtual soil from which new (raw) legal materials may be extracted.

References

Alberts, J., & Fry, B. (2015). Is Bitcoin a security? *Boston University Journal of Science & Technology Law, 21*, 1–21.

Bollen, R. (2013). The legal status of online currencies: Are Bitcoins the future? *Journal of Banking and Finance Law and Practice*, *24*, 1–38.

Brito, J., Castillo, A., & Shadab, H. B. (2014). Bitcoin financial regulation: Securities, derivatives, prediction markets, and gambling. *Columbia Science and Technology Law Review, 16*(2014), 146–221.

Colesanti, J. S. (2014). Trotting out the white horse: How the S.E.C. can handle Bitcoin's threat to American Investors. *Syracuse Law Review, 65*, 1–52.

De Filippi, P. (2014). Bitcoin: A regulatory nightmare to a libertarian dream. *Internet Policy Review, 3*(2), 1–12.

Doherty, C. (2014). Bitcoin and Bankruptcy – Understanding the newest potential commodity. *ABI Journal*, *33*, 28–33.

Doguet, J. J. (2013). The nature of the form: Legal and regulatory issues surrounding the Bitcoin digital currency system. *Louisiana Law Review, 73*(4), 1119–1153.

Fairfield, J. (2015). Bitproperty. *Southern California Law Review, 88*, 807–874.

Farmer Jr., P. H. (2014). Speculative tech: The Bitcoin legal quagmire & the need for legal innovation. *Journal of Business & Technology Law, 9*, 85–106.

Gilkes, P. (2011). *Liberty dollars may be subject to seizure.* Coin World Publications. Chicago.

Grinberg, R. (2012). Bitcoin: An innovative alternative digital currency. *Hastings Science and Technology Law Journal, 4*, 159–200.

Gwen, D., & Kroenenberg,, D. E. (2014). Bitcoins in bankruptcy: Trouble ahead for investors and bankruptcy professionals? *Pratt's Journal of Bankruptcy Law*, 112–121.

Howden, E. (2015). The crypto-currency conundrum: Regulating an uncertain future. *Emory International Law Review, 29*, 742–798.

Hughes, S. J., & Middlebrook, S. T. (2014). Regulating cryptocurrencies in The United States: Current issues and future directions. *Wm. Mitchell Law Review, 40*, 813–848.

Hughes, S. J., & Middlebrook, S. T. (2013). *Virtual uncertainty*: *Developments in the law of electronic payments and financial services.* Indiana University legal studies research paper series.

Jeans, E. D. (2015). Funny money or the fall of Fiat: Bitcoin and the forward-facing virtual currency regulation. *Journal on Telecommunications and High Technology Law, 13*, 100–127.

Kaplanov, N. M. (2012). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *Loyola Consumer Law Review, 25*, 111–171.

Kien-Meng Ly, M. (2014). Coining Bitcoin's "Legal-Bits": Examining the regulatory framework for Bitcoin and virtual currencies. *Harvard Journal of Law & Technology, 27*(2), 587–605.

Larson, J. (2015). Bitcoin: Same song, second verse, a little bit louder and little bit worse. *Michigan Tax Law, 41*, 34–37.

Maioli, C., & Perugini, M. L. (2014). *Bitcoin tra Moneta Virtuale e Commodity Finanziaria.* University of Bologna – Research Center of History of Law, Philosophy and Sociology of Law, and Computer Science and Law, pp. 1–40.

Meredith, M. W., & Kevin, V. T. (2015). Rethinking virtual currency regulation in the Bitcoin age. *Washington Law Review, 90*, 272–347.

Mittal, S.. (2013). *Is Bitcoin money? Bitcoin and alternate theories of money*. Independent Writing Project.

Nakamoto, S. (2009). *Bitcoin*: *A peer-to-peer electronic cash system*, https://bitcoin.org/bitcoin.pdf

Pacy, E. P. (2014). Tales from the cryptocurrency: On Bitcoin, square pegs, and round holes. *New England Law Review, 49*, 122–144.

Rahn, R. W. (2010). A constant unit of account. *Cato Journal, 30*(3), 521–533.

Ramasastry, A. (2014). Bitcoin: If you can't ban it, should you regulate it? The merits of legalization. *Justia.com*.

Selgin, G. (2013). *Synthetic commodity money*. The Cato Institute University of Georgia. Athens. Available at: https://bitcoin.org/bitcoin.pdf

Shadab, H. B. (2014). *Regulating Bitcoin and block chain derivatives*. Written Statement to the Commodity Futures Trading Commission, Global Markets Advisory Committee, Digital Currency Introduction.

Sonderegger, D. (2015). A regulatory and economic perplexity: Bitcoin needs just a bit of regulation. *Washington University Journal of Law & Policy, 47*(175), 175–216.

Swartz, N. D. (2014). Bursting the Bitcoin bubble: The case to regulate digital currency as a security or commodity. *Tulane Journal Technology & Intellectual Property, 17*, 320–335.

Trautman, L. (2014). Virtual currencies Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law and Technology* 20. Available at http://jolt.richmond.edu/v20i4/article13.pdf

Vaishampayan, D. S. (2013). Bitcoins are private money in Germany. *Wall Street Journal*, *The Tell* (blog).

Wallace, B.. (2011). The rise and fall of Bitcoin. *Wired Magazine*, San Francisco.

Weber, B. (2014). Can Bitcoin compete with money? *Journal of Peer Production* 4. Available at http://peerproduction.net/issues/issue-4-value-and-currency/invited-comments/can-bitcoincompete-with-money/

White, L. H. (2014). *The troubling suppression of competition from alternative monies: The cases of the liberty dollar and E-gold*. George Mason University, Department of Economics, Working paper no. 6, pp. 1–30.

Ziskina, J. (2015). The other side of the coin: The Fec's move to approve cryptocurrency's use and deny its viability. *Washington Journal of Law Technology and Arts, 10*, 306–327.

6

M-Payments: How Much Regulation Is Appropriate? Learning from the Global Experience

Elisabetta Cervone

Abstract The author offers a roadmap approach to regulating mobile payments (hereinafter "m-payments") worldwide. This chapter draws the attention to the regulatory restrictions and/or regulatory uncertainty which govern m-payments and which are the most formidable barriers to expanding m-payments to the mass market. It focuses on the pioneering—mostly unregulated—model M-Pesa in Kenya, on one side, and on the US legal and regulatory framework, on the other. The lesson from the global experience so far is that it is too early for regulators to assume that there is an established or "orthodox" method of regulating m-payments. However, the author concludes that—as a roadmap approach to regulating m-payments worldwide—a functional rather than institutional approach is strongly recommended.

E. Cervone (✉)
World Bank, Finance and Markets Global Practice, Payment Systems Development Group
University of Milan, Department of international, juridical and historical-political studies, Italy

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_6

Introduction

M-payments are playing an increasingly prominent role in widening the offering of payment services and achievement of broader access to payment services.[1] Given the relatively high cost of a bank account—minimum balance, service charges, full know your customer (hereinafter "KYC") requirements and travel time to a branch—and the easy, low cost and increasingly universal access to mobile services, the mobile operator model arguably is highly effective in bringing informal cash transactions into the formal financial system, expanding access to financial services.

The recent growth of m-payments has been contributing to enhance financial inclusion.[2] It has been proved that innovation often occurs where the need for change is greatest.[3] In developing countries, where the traditional payment infrastructure is lacking, the fast take-up of new technology is enabling payment services to be provided to the unbanked. By the later part of the 2000s, the main action in m-payments was occurring in developing and less-developed countries, from Kenya, to Brazil, the Philippines, South Africa, where m-payments are really attractive to unbanked and underbanked people because of the lack of bank branches.

Developed economies are so far behind developing countries.[4] While in less-developed countries loss aversion may be slow and they may be

[1] M-payments can be defined as payments initiated and transmitted by access devices that are connected to mobile communication networks. Committee on Payment and Settlement Systems (CPSS) *Innovations in Retail Payments* (Bank for International Settlements, 2012), 19. On m-payments in general, see Thomas-Frank Dapp et al., *The Future Of* (*Mobile*) *Payments*: *New* (*Online*) *Players Competing With Banks* (Frankfurt am Main, Germany: Deutsche Bank Research, 2012); on m-payments in the European Union, European Commission, *Green Paper*: *Towards An Integrated European Market For Card*, *Internet And M-Payments* (Brussels: EC, 2012).

[2] M-payments have allowed millions of people who are otherwise excluded from the formal financial system to perform financial transactions relatively cheaply, securely and reliably. Financial inclusion has become a subject of growing interest for researchers, policymakers and other financial sector stakeholders.

[3] In addition, in microfinance it is well known that the poor have limited liability since they do not have the possibility to lose anything. Thus, in poor countries loss aversion may be slow and they may be more open to experimenting with new models of m-payments, as in Africa, for example, where there are few banks, poor physical infrastructures and a rural population often dependent on remittances from the city.

[4] In the USA, only recently, a system by Apple-Pay has been enacted, which allows iPhone users to pay at the checkout counter simply by holding their phone to a receiver for a few seconds. See http://time.com/money/3328891/apple-pay-iphone-global-mobile-payments/.

more open to experimenting with new models of payments, in developed countries there is generally high consumer satisfaction with existing retail payment options, which are reliable, familiar and trusted.

Apart from different economic, social and cultural backgrounds, an enabling national, legal and regulatory environment is essential to ensure widespread use of m-payments.

Regulatory authorities, in advanced as well as less-developed economies, are faced with great challenges in regulating m-payments, especially because m-payment technology is in the early stages of its development. The tension between, on one hand, the desire to innovate and to develop policy environments that will enable and support innovative models of payments and dedicated to pursuing a more open and competitive market and, on the other hand, the need to ensure the stability and safety of the national payments system and protect consumers, with particular emphasis on those who are considered financially vulnerable, has left many regulators cautious on the most prudent path to take.[5]

Regulators differ in their attitude towards governing m-payments. In some countries, innovation is preceding legislation: m-payments remain outside the scope of banking regulation and a "test-and-see" approach is adopted to permit experimentation in the field. In other countries, instead of a "test-and-see" approach, m-payments remain governed by the same legal framework that applies to traditional banking services.

[5] There is considerable work done in this area in the recent past including the "Retail Payments Package" produced by the World Bank Payment System Developing Group, which offers guidance and tools, including: (i) "Developing A Comprehensive National Retail Payments Strategy", which aims to provide public authorities and market participants with detailed guidance on how to develop and implement a comprehensive, strategic retail payments reform; (ii) "A Practical Guide For Retail Payments Stocktaking", which identifies a methodology for undertaking a detailed stocktaking of a country's retail payments landscape; (iii) "From Remittances To M-Payments: Understanding 'Alternative' Means Of Payment Within The Common Framework Of Retail Payments System Regulation", which explores the development of a normative framework to underpin an efficient retail payments industry, including the so-called innovative payment mechanisms; (iv) "Innovations In Retail Payments Worldwide: A Snapshot: Outcomes Of The Global Survey On Innovations In Retail Payments Instruments And Methods 2010", which presents the results of the first World Bank survey among central banks that collected information on innovative retail payment products and programs. Available at: http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/0,,contentMDK:23252983~pagePK:210058~piPK:210062~theSitePK:282885,00.html.

While the "test-and-see" approach, adopted in Kenya, is much more flexible and encourages innovation, it potentially exposes m-payments customers to significant risks. The second approach, adopted in the USA, applies the overly complex, legal and regulatory framework for traditional banking services to m-payments, in this way discouraging innovation and thus limiting the ability of m-payments to reach previously financially excluded groups.

Drawing a comparison between the US framework on one side and the M-Pesa in Kenya on the other, the lesson from the global experience so far is that it is too early for regulators to assume that there is an established or "orthodox" method of regulating m-payments. There is still a need to experiment with different business approaches to learn how each performs in different market circumstances. However, as a roadmap approach to regulating m-payments worldwide, a functional rather than institutional approach is strongly recommended across countries. That would be the best way to manage risk without stifling innovation.[6]

Current Approaches to Regulate M-Payments: From Kenya to the USA

Kenya and the Developing Countries: When Innovation Precedes Legislation

Adoption of m-payments has been varied across developing economies' markets. Among some of the reasons are differences in the economic, regulatory and banking infrastructure of countries.

Kenya, Tanzania and Ghana have limited infrastructure for banking, making m-payments appealing to consumers. In contrast, banking infrastructure is well established in countries like India. Governments in Kenya (as we will see) and the Philippines have adopted mobile operator-friendly regulations that allow mobile operators to take on many of the banking operations. However, South Africa, India, Bangladesh, Tanzania

[6] On risk management in m-payments, see Andrew James Lake, *Risk Management In Mobile Money: Observed Risks And Proposed Mitigants For Mobile Money Operators*, Swiss Confederation 2013.

and Uganda require a bank's involvement in any banking transaction. In India, in particular, there are more than ten major mobile operators that make interoperability of payments among them a challenge. In contrast, Safaricom in Kenya had a dominant market share that made it a de facto monopoly making it easier to establish its payment service as a standard in the country.[7]

While, as a result of these differences, there could not be successful imports of payment models from one country to another, the m-payments provider M-Pesa in Kenya has been often taken as a good model to emulate.

When M-Pesa was introduced in Kenya, it had no association with the formal banking sector and m-payments customers there were exempt from the documentation requirements imposed by banks. It was developed by the mobile operator Vodafone and launched commercially by its Kenyan affiliate Safaricom in 2007. It offers an electronic payment and store of value system accessible through mobile phones: once assigned an individual electronic money (hereinafter "e-money") account linked to their mobile phone number, consumers can deposit and withdraw cash to and from their accounts by exchanging cash for electronic value.[8] They can then transfer funds to other M-Pesa users and even non-registered users.[9]

[7] In this article, the expression "payment services" is used to mean services enabling cash deposits and withdrawals, execution of payment transactions, issuing and/or acquisition of payment instruments, money remittances and any other services functional to the transfer of money; it also includes the issuance of e-money and e-money instruments. The expression "payment instrument" means any instrument, whether tangible or intangible, that enables a person to obtain money, goods or services or to otherwise make payment or transfer money. These include, but are not limited to, cheques, funds transfers initiated by any paper or paperless device (such as automated teller machines, points of sale, internet, telephone), payment cards (including those involving storage of e-money) and money remittances.

[8] The expression "electronic money", as used in this chapter, means monetary value represented by a claim on the issuer, which is, (i) stored on an payment device such as chip, prepaid cards, mobile phones or on computer systems as a non-traditional account with a banking or non-banking entity; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; and (iii) accepted as a means of payment by persons other than the issuer.

[9] The rapid growth of M-Pesa caught everyone by surprise. In just one year M-Pesa had 1 million clients. By early 2012 M-Pesa had 15 million registered users, a network of over 35,000 cash-in and cash-out agents, and a transaction volume of USD665 million per month. Mark Okuttah, "M-Pesa Drives Safaricom as Profit Declines to Sh12.8bn." *Business Daily*, posted 10 May 2012. http://www.businessdailyafrica.com/Corporate+News/MPesa+drives+Safaricom+as+profit+declines+/-/539550/1403606/-/35hl1b/-/index.html.

Starting as a popular platform on which people could send domestic remittances across distances at a low cost, M-Pesa functionality broadened as users began to leave funds in reserve on the platform, creating a kind of short-term savings device. With the success of Safaricom, many players quickly entered the field: as of December 2010, there were at least seven systems offering some type of bank account access via mobile phone. Most of these function on partially integrated mobile systems, where customers are first required to establish a traditional account in a physical bank, through which they could gain access via a mobile phone. On the other hand, M-KESHO, a joint-venture between Safaricom and Equity Bank, currently offers a fully integrated mobile savings system, where customers can sign up directly via Safaricom agents.

The discussion of M-Pesa needs to consider its relative uniqueness in terms of favourable market and regulatory conditions.

The prominent role of a telecommunication company in providing payment services allowed a single provider to capture significant economies of scale in a way that might be difficult to replicate (or not desirable) in other settings. M-Pesa calls for a big player with a dominant market share and capacity to attract together the ecosystem (banks and agents) and aggregate transaction volumes. Generally, though not always, the largest mobile operator in a country is in the strongest position to become the dominant player in m-payments. Incumbent mobile operators have a widely recognized brand, a distribution network which includes a large number of retail outlets in their territory and experience with a high volume transactional business model.

In addition, there were nearly absent regulatory conditions. M-payments in Kenya evolved quickly in a largely undefined regulatory space.[10] Kenya had no laws, regulations or policies that were directly applicable to e-money transactions.[11] However, to ensure compliance with standard banking practices, Safaricom consulted the Central Bank of Kenya in 2006. Since then the Central Bank has continued to pro-

[10] Simone Di Castri et al., *Consumer Protection Diagnostic Study* (Kenya. Nairobi: Financial Sector Deepening Kenya, 2011), p. 11.

[11] Rasheda Sultana, *Mobile Banking: Overview Of Regulatory Framework In Emerging Markets* (Bangladesh: Grameenphone Ltd., 2009).

vide oversight and guidance.[12] Through collaboration and innovation, the Central Bank and Safaricom have addressed emerging challenges vis-à-vis the introduction of m-payments as well as consumer protection initiatives.[13] Safaricom, in particular, developed its own approach to disclosure, fair conduct and dispute resolution.[14] Likely as a result of this effective collaboration between Safaricom and the Central Bank, M-Pesa emerged with consumer-friendly policies in spite of the absence of consumer protection laws.

M-Payments in the USA: A Legal and Regulatory Maze

While M-Pesa in Kenya developed in the absence—or nearly absence—of regulation, currently m-payments in the USA are subjected to a multitude of regulators and regulations.[15]

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) created the *Consumer Financial Protection Bureau* (CFPB), which plays a vital role in the furtherance of m-payments regulations. Under the Act, the CFPB has authority to regulate consumer financial products and services under federal consumer financial law.[16] More specifically, the CFPB has enhanced authority to regulate "unfair, deceptive, or abusive acts or practices".[17]

In addition to the newly created CFPB, other financial regulatory agencies have (limited) regulatory oversight on m-payments: the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve System (FRS), the National Credit Union Association (NCUA), the Office of

[12] Di Castri, ibid., 11.

[13] Sultana, ibid.

[14] Di Castri, ibid., 13.

[15] For a description of the current m-payments ecosystem in the USA, see: Darin Continie et al., *M-Payments In The United States: Mapping The Road Ahead* (Boston, MA: Federal Reserve Bank of Boston, Federal Reserve Bank of Atlanta, 2011); Mobile Payments Industry Workgroup (MPIWG), *The US Regulatory Landscape For Mobile Payments* (Federal Reserve Bank of Atlanta and Federal Reserve Bank of Boston, 2012), available at https://www.bostonfed.org/bankinfo/payment-strategies/publications/2012/us-regulatory-landscape-for-mobile-payments.pdf.

[16] 12 U.S.C. § 5511 (Dodd-Frank Act § 1021).

[17] 12 U.S. Code § 5531.

the Comptroller of the Currency (OCC), the Federal Communications Commission (FCC), the Federal Trade Commission (FTC) and the Financial Crimes Enforcement Network (FinCEN).[18]

It is generally understood that, in the USA, current laws and regulations on underlying payment methods and instruments (credit, debit, prepaid) are applicable to m-payments.

Applicable to the electronic transfer of funds, the Electronic Fund Transfer Act (EFTA) protects consumers against losses accrued as a result of an unauthorized transaction. It is not clear if Regulation E, which implements the EFTA, is applicable to mobile operators. Regulation E defines an electronic fund transfer as "any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account." This definition includes transfers that take place via mediums such as direct deposits, direct withdrawals, debit card transactions and automated teller machine (ATM) transactions. According to this definition of an electronic funds transfer, Regulation E, therefore, clearly applies to m-payments when the transaction is made from a consumer's account through an electronic funds transfer. For example, a financial institution, such as a bank, must

[18] The FDIC governs part of m-payments by supervising banks and assuring that they comply with consumer protection laws, such as the Fair Credit Reporting Act, the Fair Credit Billing Act, and the Truth-In-Lending Act. The FRS, although serving as the nation's central bank, has the responsibility, inter alia, to supervise and govern banks, ensuring the payment system remains stable and safe. The NCUA regulates federal credit unions and the OCC regulates national banks and federal savings associations by ensuring that they operate in a safe and sound manner, provide fair access to financial services, treat customers fairly, and comply with applicable laws and regulations. The FCC regulates interstate and international communications by radio, television, wire, satellite and cable. Because one of the goals of the FCC is to regulate homeland security through communications, the FCC has an interest in regulating the security and privacy data of m-payments, although FCC's role as a m-payments regulator needs to be clarified because it does not have direct regulatory authority. In contrast, the FTC has direct authority over several participants in the m-payment ecosystem, including operating system developers, application developers, handset manufacturers, advertising companies, telecommunication providers and even companies offering bill-to-carrier options. The FinCEN also is an agency touching m-payments. As a division of the US Department of Treasury, the FinCEN's purpose is to enhance the integrity of financial systems by facilitating the detection and deterrence of financial crime. Because financial crimes involve money laundering, FinCEN issued the *Prepaid Access Final Rule*, requiring prepaid access providers and sellers to file suspicious activity reports, retrieve and hold transactional and customer information, and effectuate an anti-money laundering program.

comply with Regulation E when a consumer uses a mobile phone to make a payment via his or her debit card, which is linked to the phone. The application of Regulation E is much less clear, however, as it applies to non-financial institutions, including many new m-payment participants. Mobile operators, traditionally non-financial institutions, could be subject to Regulation E if they issue debit cards to consumers without holding the consumer's account and offer electronic funds transfers without an agreement with the account-holding institution. To make this scenario possible, the Federal Reserve Board would have to determine that m-payment data is an electronic funds transfer when transferred via a mobile operator's network, and they would have to classify a mobile phone as an access point.

Another regulation which may be applied to m-payments is Regulation Z, promulgated by the Federal Reserve Board to specifically govern credit card transactions. Regulation Z resolves issues of liability for unauthorized transaction or responsibility for billing errors. Additionally, Regulation Z requires creditors, including credit card issuers, to make initial disclosures of certain items (such as financial charges, billing rights and interest rates) and to make subsequent disclosures of certain items (such as those dealing with annual statements and the availability of additional credit accessing devices). Although Regulation Z clearly provides guidance for traditional participants dealing in credit card transactions, its application to new m-payment participants is unclear, much like Regulation E. The Federal Reserve Board, for example, has not clarified whether mobile operators are subject to Regulation Z when they advance credit to subscribers who purchase ring tones or games.

The Gramm-Leach-Bliley Act (GLBA) may also be applied to m-payments. The GLBA governs the privacy of customers' information. Title V requires financial institutions to establish standards that safeguard customers' records, preventing any unauthorized access to such information. Additionally, Title V requires financial institutions to disclose to the customer, both initially and annually thereafter, the institution's policies regarding the disclosure of customers' non-public personal information. Although the application of the GLBA is clear when applied to banks, its application to mobile operators is not so clear.

The Bank Secrecy Act, as amended by the US PATRIOT Act,[19] requires the collection of identity information to combat money laundering. The PATRIOT Act requires financial institutions to not only establish procedures to detect money laundering, but it also requires financial institutions to submit suspicious activity reports when it suspects a transaction involves money laundering. Although anti-money laundering (hereinafter "AML") regulations clearly apply to banks, AML regulators have not applied them to m-payments participants. Consequently, AML regulations can be circumvented when terrorists use a m-payment platform to transfer funds obtained illegally.

The Federal Trade Commission Act[20] prohibits, inter alia, "unfair or deceptive acts or practices in or affecting commerce". This Act applies to nearly all persons and entities engaged in commerce, including then m-payments when a person utilizes a mobile phone to engage in commerce.

The Dodd-Frank Act adds the word "abusive" by prohibiting "any unfair, deceptive, or abusive act or practice". Thus, m-payments could possibly fall under CFPB authority when transactions or purchases fall under the above language. While there is no one clear regulator who is in charge of all m-payments, the CFPB, which has broad authority to prohibit unfair, deceptive or abusive practices or acts, is most likely to be the agency to govern m-payments.

Supporting an Enabling Regulatory Framework for M-Payments

We examined two different approaches to regulate m-payments in Kenya and the USA While both the approaches failed in properly addressing risks in m-payments activities at the beginning, they took in due consideration the fundamental link between regulation and innovation and the fact that there is not an orthodox way to discipline m-payments.

[19] The United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act.

[20] 15 USC 45, section 5.

In Kenya, they experimented and learned. Since the implementation of M-Pesa, the Central Bank has made some changes to the regulatory framework for m-payments. In 2010, the Central Bank enacted *Guidelines on Agent Banking* to prescribe the manner in which agents should conduct business in Kenya so that the supervision, safety and soundness of the banking sector is ensured. In 2011, the Bank issued the *National Payment System Act* to supervise payment systems and to more clearly articulate which firms will be defined as payment service providers[21] (hereinafter "PSPs") and regulated accordingly. Through the *National Payment System Act*, a broader regulatory and consumer protection framework for the m-payments industry is now beginning to unfold in Kenya.

In the USA, regulators in 2012 concluded that there is no immediate need to issue additional regulations or update existing ones in order to discipline m-payments, at least until the stage of maturity of m-payments technology is in its infancy stage.[22]

Understanding what the most supporting regulatory framework is for m-payments constitutes a great challenge for regulators.

In many countries, significant regulatory barriers persist that constrain an operator's ability to build sustainable m-payments services. While regulations governing traditional payment methods might be generally applied to emerging m-payment methods, such legal and regulatory frameworks could be complex and inadequate to ensure safety and efficiency of the payment system and consumer protection. There is a need to understanding what is effectively innovative in these instruments so that requires different regulatory tools and what, instead, is just an implementation of existing schemes already covered by retail payments regulations. Regulation directly affects the innovative process, while innovation and technical change have significant impacts on regulation. However, if

[21] In this chapter, the term "payment service provider" is used to mean an entity that provides payment services.

[22] To address the issue of whether the current regulations governing traditional payment are insufficient to cover m-payments, the Federal Reserve Banks of Boston and Atlanta in 2010 convened a group of selected key players in m-payments, the Mobile Payment Industry Workgroup (MPIW), to discuss the potential gaps in regulations touching and concerning m-payments and provide regulatory guidance. The members of the MPIW, FCC, FTC and other members of federal and state banking agencies met in 2012.

regulators take simply a "wait-and-see" approach with m-payment innovations, without any regulatory intervention, the result is significant risks being passed on to consumers.

Relevant stakeholders are often operating cross-border (e.g. Safaricom is the Kenyan subsidiary of Vodafone). As geographic borders lose their relevance, m-payments initiated in Kenya are likely to migrate to the USA and vice versa. For example, Kipochi, a web-based wallet service, has linked M-Pesa with Bitcoins, enabling Kenyans to send and receive value beyond their borders, where M-Pesa is unavailable; this combination of services enables a flow of funds both within and beyond the country. In the interest of preserving the integrity and safety of domestic and cross-border retail payment systems, industry stakeholders, policymakers and regulators should act cooperatively.

While harmonization of all regulations across countries is not possible, given their different economic, social and cultural backgrounds, countries should continue to pursue greater compatibility among regulations in the interest of both economic efficiency and innovation. Regulatory differences can not only constitute barriers to market access, but also hinder technical advance and technology diffusion, as in the case of conflicting competition, financial and intellectual property laws. There is a need for an enabling and predictable legal and regulatory framework for m-payments, which has to be consistent across countries and enforced by the authorities in a predictable way.

Even though m-payments can be understood—and have to be understood—and analyzed within the general framework of the retail payments system, there are some legal and regulatory measures—in common with other innovative means of payments provided by non-bank actors—which may be more conducive to m-payments and which governments are recommended to adopt.[23]

First, access to m-payments, and the national payment system in general, for non-bank PSPs needs to be facilitated.

M-payments differ from traditional payment services, which are mainly account-based payment services, dominated by banks and non-bank

[23] On the role of non-banks in payment services, see Committee on Payments and Market Infrastructures, *Non-Banks In Retail Payments*, Bank for International Settlements, 2014.

financial institutions. In the provision of m-payments new actors—including mobile operators and third-party agents acting on their behalf—are introduced in the traditional landscape and the payer is not anymore required to hold a bank account to make a payment. However, some financial sector authorities refuse to license non-banks as PSPs and in many countries—such as in South Africa, India, Bangladesh, Tanzania and Uganda—banks continue to have an active role in m-payments.[24]

Enhancing access to payment services to non-banks would also imply permitting non-banks to issue e-money. However, with the growth of e-money products and the aggregate value of funds stored in the underlying e-money accounts, regulators are paying increasing attention to the risk of misuse or loss of these customer funds, which are typically not comprised in deposit guarantee schemes.[25] Measures like trust funds or segregation of funds can be used to mitigate risk.[26]

The regulatory approach adopted in the European Union should be seen as a model.[27] The revised Directive on Payment Services (hereinafter "PSD2") widens the scope of the Directive on Payment Services (PSD) by covering new services and players as well as by extending the scope

[24] Established banks can embark on m-payments with relatively low risk and cost. Unlike mobile operators, banks can exploit the arrangement of cash-in/cash-out points incrementally, since they already have an existing product range, a branch network and marketing channels. A bank could start by signing up a few cash-in/cash-out points around a few branches and over time build a substantial base. Above all, banks are already fully prudentially regulated and supervised.

[25] While in a pure "bank-led model", a bank (or other licensed deposit-taking institution) holds the customer funds, in "non-bank-led" models, the customer is not required to have a bank account. Individual payment transactions occur entirely within the mobile operator. The funds in transit are matched by a deposit in a pooled account with one or more banks (when the issuance of e-money for cash is involved). However, since the PSP is not providing credit and not providing a deposit-taking function, customer funds are typically not comprised in deposit guarantee schemes.

[26] For example, India and the United States, have introduced measures to protect customer funds if the issuer of prepaid payment instruments becomes insolvent. Committee on Payments and Market Infrastructures (CPMI) and the World Bank Group (2015 *Consultative Report On Payment Aspects Of Financial Inclusion* (so-called "PAFI Report", 36). The report examines demand- and supply-side factors affecting financial inclusion in the context of payment systems and services and suggests measures to address these issues.

[27] See Chap. 4.

of existing services, enabling their access to payment accounts.[28] While under the current PSD m-payments are not covered, under the PSD2 the purchase of physical goods and services through a mobile operator falls within the scope of the Directive.

Second, a functional rather than institutional approach to regulation should be adopted.

This implies a non-discriminatory legal and regulatory framework, which is one that is equally applicable to different types of PSPs insofar as they are providing equivalent services. Regulating payments solely by type of entity may make regulation less effective and distort markets where regulation allows only certain types of providers, most often banks, to operate in the m-payments. A functional rather than an institutional approach to regulation of payment services—where equivalent services are regulated the same way, regardless of type of entity providing the service and delivery channel—helps to level the playing field among different types of PSPs and promotes competition on a fair and equitable basis. M-payments might deserve different regulatory treatment depending on the different ways the service is organized, the legal schemes which are adopted, the contractual allocation of risk and the clearing and settlement of transactions. This approach has been followed in the EU, with the adoption of the PSD, the PSD2 and the E-money Directive.[29]

M-payments should be understood as three entirely separable activities: (i) there are the real-time transactional platforms which perform the fairly mechanical functions of account management and transaction authorization; (ii) there is the intermediation of funds, which consists of the investment of the funds that are backing those accounts, channeling the resources

[28] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance). In October 2015 the European Parliament adopted the revised Directive on Payment Services (PSD2). Following the Parliament's vote, the Directive will be formally adopted by the EU Council of Ministers. European Parliament legislative resolution of 8 October 2015 on the proposal for a directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC (COM(2013)0547–C7-0230/2013–2013/0264(COD)).

[29] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance).

back to productive opportunities in the wider economy; (iii) there is the cash-in/cash-out business, which consists of helping customers exchange between two forms of money (cash and electronic value) against the store's own inventory of the same two forms of money. The more these three businesses are bound into one by regulation, the harder it could be to create a m-payment network. Regulators bind the account management and intermediation businesses whenever they require that payment platforms be operated (directly or indirectly) only by banks. Allowing non-banks to be e-money issuers is a good way of unbundling these two businesses, permitting non-banks to engage in the accounts management business as long as the banks retain the higher-risk intermediation business.

Third, a proportional legal and regulatory approach for m-payments should be pursued.

Such approach is one that is not overly restrictive and burdensome relative to the possible issues it is designed to address or to the number and value of transfers involved. M-payments can pose risks to the financial system—products may be used to launder money or finance terrorism—but they also provide the important public policy goal of financial inclusion and, on an individual basis, are often very low-value transactions. If too stringent and not proportional to the risks at hand, AML regulation can create barriers for senders to use regulated payment services, discourage non-banks from offering payment services and hamper the growth of new technologies that facilitate the use of m-payments and potentially lower costs. Adopting a risk-based approach would simplify the KYC requirements for basic, no-frills accounts. Such an approach has already been adopted in Mexico, where providers placed a limit on size of transactions per day before requiring increased identification. Less stringent KYC requirements might make accessing the financial system more approachable for the unbanked and underbanked.[30]

[30] Several financial regulators still impose account-opening requirements that the poor cannot meet, which represents a conservative approach to interpreting the standards of the Financial Action Task Force (FATF) that does not take into account the risk-based approach recommended by the FATF, the FATF guidelines on financial inclusion and the experience of progressive countries that have adopted alternative and simplified opening procedures to overcome the obstacle represented by traditional identification criteria. Strict KYC rules employed in some markets place prohibitive costs on PSPs. For more information on the FATF risk-based approach, see FATF, *Guidance For A Risk-Based Approach. The Banking Sector*, FATF/OECD, 2014.

Fourth, transparency and adequate consumer protection measures need to be promoted.

The fees, terms and conditions associated with transaction account services and/or individual payment instruments can be quite complex, particularly for first-time customers (as m-payments users often are).[31] Other major concerns are on data security (sensitive information transferred during a m-payment transaction can be intercepted, stolen or used in an unauthorized manner), on the inadequacy of privacy regulations to protect m-payment transactions and on dispute resolution (i.e. in case of fraudulent or unauthorized charges in m-payments).

Many jurisdictions have only recently adopted financial consumer protection frameworks. Few have regulations relevant to m-payments.[32] These regulations typically address fundamental consumer protection principles such as transparency and disclosure, fair treatment and recourse mechanisms for banking products such as loans and deposits.[33] However, since the regulations tend not to apply to non-bank PSPs, consumer protection varies depending on the source of funds used to make the payment. Because m-payments often involve more than one payment source, whether consumers have statutory protection or not depends on the underlying source of the m-payment.

Fifth, cooperative oversight arrangements are necessary.

The provisioning of m-payments can go from the extreme of being provided by telecommunications operators without any direct involvement of a bank, through being provided in strict cooperation with the banking sector, at least for clearing and settlement, up to situations where banks outsource such services to a telecommunications operator or even use the operator as nothing more than a communication channel, with the service fully provided by banks. This may involve coopera-

[31] The European Union and Turkey have introduced requirements for the transparency and comparability of account fees and payment services.

[32] Recently, when the Consultative Group to Assist the Poor (CGAP) analyzed financial consumer protection in the Europe/Central Asia region (i.e., Albania, Armenia, Azerbaijan, Bosnia, Georgia, Kazakhstan, Kosovo, Kyrgyz Republic, Macedonia, Russia, Serbia, and Tajikistan), they found that most of the countries did not begin to develop rules until 2008. Consultative Group to Assist the Poor, *Financial Consumer Protection Regulation In Europe/Central Asia* (CGAP, 2012).

[33] Consultative Group to Assist the Poor, ibid.

tive oversight among regulatory agencies such as the telecommunications regulator, the competition or consumer protection authority. While one national agency should have primary responsibility over m-payments, this primary agency should act in coordination and cooperation with the other numerous regulatory agencies that have responsibility over different aspects of m-payment transactions. In an effort to enhance dialogue and cooperation among industry stakeholders, the US Federal Reserve has convened the M-payments Industry Workgroup and the European Central Bank supervises the European Payments Council. These working groups share data and research and develop principles.

Sixth, mobile operators must have adequate access to domestic payment infrastructures.

Mobile operators usually require the use of national payment systems in order to process money transfers. Non-bank PSPs such as mobile operators often have only indirect access to payment systems and depend on direct participants, usually banks, to provide them with the required services (i.e. bank accounts, settlement with collecting/paying agents nationally). In some countries, non-bank PSPs struggle to even obtain indirect access to the national payments system, because direct participants refuse to serve non-bank PSPs.

Beside adequate access to domestic payment infrastructures, such infrastructures need to be interoperable. M-payments users will fully benefit from competition, freedom of choice and more efficient payment operations if interoperability and some level of interconnection among competing m-payments schemes is achieved. M-payment ecosystems are built on both interoperable technologies (e.g. short messaging service or SMS), which have shared protocols to permit interaction among computer systems, and proprietary technologies (e.g. the "Google Wallet" software application or a mobile device's operating system such as iOS 7). While regulation needs to enable interoperability by facilitating strategic partnerships across industries and promoting competition between firms, it should not be so strict because it would risk stifling innovation and is not appropriate for keeping pace with technology, fraud and market developments. Instead, interoperability among m-payment solutions should be better ensured by standardization through technical requirements and best practices. The standards in question should be preferably

open standards (which are freely available and are developed and maintained via a collaborative and consensus-driven process) rather than proprietary standards (that are privately owned and generally not approved by standard-setting bodies).[34]

Lastly, regulation of third-party service providers, such as agents and outsourcing, is almost absent in most jurisdictions. In order to operate efficiently and to enhance the potential for financial inclusion, m-payments need a network of agents (such as merchants or post offices), as an alternative, or more often in addition, to bank branches.[35]

In a number of countries it is still difficult, if not impossible, for mobile operators to appoint agents. Specifically, regulations that PSPs from engaging third-party agents to carry out customer acquisition functions and cash services create a significant barrier to commercially viable implementation models. There is often misunderstanding of the risks that moving payments outside of bank branches pose, risks that would be properly managed and mitigated by ensuring clear liability rules. Full liability for acts done by third parties should rest with the principal and such attribution of responsibility should be clearly stated in the national payments system law.

Another regulatory aspect that needs particular attention when providing payment services through third parties is the one related to exclusivity agreements. Regulators should consider prohibiting exclusivity agreements between PSPs (including mobile operators offering payment services) and their agents or limit the period for which they may be imposed. Exclusivity agreements between PSPs and their agents prohibit agents from offering the services of any other PSP, thereby reducing capacity of other PSPs to expand their network, and consequently reducing the range

[34] Given the specificity of m-payments, standardization should address the issue of portability of m-payment applications (i.e. how payment applications follow consumers when they change mobile operators). Standardization of the various components (e.g. protocols, interfaces, applications, services) needs to be carried out thoroughly in order to minimize the risk of foreclosure of potential competitors or innovation.

[35] Brazil has made payments access points significantly more available throughout the country through agent banking/business correspondents. The Central Bank started developing the current model in the late 1990s and that model has now become a permanent part of its agenda. Today, business correspondents account for more than half of all payments access points in the country. Other countries in Latin America and the Caribbean, Russia and India are following suit.

of products available to m-payment users in one given access point, or making accessing certain PSPs less convenient and possibly more costly. By restricting this choice, exclusivity agreements may result in a de facto monopoly.

Conclusions

The full potential of m-payments is yet to be realized in the current regulatory regime, but likely to flourish if specific barriers and/or regulatory uncertainty are removed from existing regulations in many countries. An enabling legal and regulatory framework underpins financial inclusion by effectively addressing all relevant risks and by protecting consumers, while at the same time fostering innovation and competition.

Learning from the experiences in both Kenya and the USA, regulatory reforms for m-payments are necessary. Regulations governing m-payments are "fragmented" and confusing. There is a need of avoiding overlapping or inconsistent regulations: multiple laws (such as legislation on electronic fund transfers, on e-money, on consumer protection, on AML, data protection, e-commerce, IT) and authorities are generally involved. In addition, existing regulations seem not to be sufficient to properly manage risks and consumer protection.

Issues regarding the application of existing regulations to m-payments can adequately be resolved or at least mitigated if an enabling legal and regulatory framework is developed in a way that would encourage—not impede—innovation.

The answer to the question, in the title of this chapter, "how much regulation is appropriate" should be the result of balancing public policy objectives, which may not always point in the same direction. *On the one hand*, encouraging access and competition increase financial inclusion, while *on the other hand*, other public policy objectives such as financial integrity and consumer protection favour potentially burdensome regulation. An appropriate balance should be achieved. Policymakers and regulators should build the capacity to engage and maintain an active, experimental approach, shaping the regulatory environment so as to enable experimentation and eventually increase their control and oversight through different

phases of market development, carefully sequencing their proportionate response to risks.

In any case, it is vital to promote a legal and regulatory framework that is sound, predictable, non-discriminatory and commensurate to the level of risk. It is also equally important that competition is enhanced by encouraging non-banks to enter the market. Regulators should understand and encourage non-bank providers. Beside the essential role of banks, non-banks play also vital roles (such as hosts of payment platforms, providers of retail payment instruments, managers of agent networks). The degree to which m-payments is capturing the non-banked market clearly differs across economies and it will depend on the market as to which is more suitable.

Consistent standards of regulations across jurisdictions should be encouraged, calling for an efficient and effective cooperation among regulatory authorities. The peculiarity of the m-payments ecosystem has made in evidence the importance of all relevant stakeholders' participation in developing an enabling legal and regulatory framework for m-payments. In Kenya, the telecommunications operator has been operating under the informal guidance and supervision of the Central Bank. In Kenya, both the government and the Central Bank played an important role in facilitating access to m-payments. In the USA, relevant regulatory agencies have been participating and discussing legal and policy options through the MPIW.

It is still too early to know which path is most likely to succeed in the long run. A m-payments scheme may be successful in one country, but will not necessarily perform as well in other countries. The industry as a whole is still working to demonstrate the viability of different models and partnership arrangements. M-Pesa in Kenya is a brilliant story about the power of m-payments. However, it remains a single story and one has to wonder whether this is really a replicable model.

The PSD may serve as a benchmark. The Directive, which provides the legal foundation for the creation of an EU-wide single market for payments, seeks to improve competition by opening up payment markets to new entrants, differing from banks, thus fostering greater efficiency and cost-reduction. The draft revised PSD (PSD2) would further extend the scope of the PSD to cover new services and service providers enabling

access to consumer accounts, thus aiming at bringing the legislation up to speed with developments in m-payments.

Ongoing sharing with peer regulators about emerging experiences will help the learning process. This chapter supports a policy road map that focuses on specific regulatory changes—driven by a functional rather than institutional regulatory approach—and parallel development of appropriate oversight capacity, based on mutual regulatory learning. This approach, which has been discussed for m-payments, can—and should—be applied to any other innovative means of payments.

References

Committee on Payments and Market Infrastructures (CPMI) and World Bank Group. (2015). *Consultative report on payment aspects of financial inclusion*. Bank for International Settlements and World Bank Group. Washington, DC.

Committee on Payments and Market Infrastructures (CPMI). (2014). *Non-banks in retail payments.* Bank for International Settlements. Basel.

Committee on Payment and Settlement Systems (CPSS). (2012). *Innovations in retail payments.* Bank for International Settlements.

Consultative Group to Assist the Poor (CGAP). (2012). *Financial consumer protection regulation in Europe/Central Asia.* Washington, DC.

Continie, D., et al. (2012). *M-payments in the United States*: *Mapping the road ahead.* Boston, MA: Federal Reserve Bank of Boston, Federal Reserve Bank of Atlanta.

Dapp, T.-F. (2012). *The future of (mobile) payments: New (online) players competing with banks*. Frankfurt am Main, Germany: Deutsche Bank Research.

Di Castri, S., et al. (2011). Consumer protection diagnostic study. Nairobi, Kenya: Financial Sector Deepening Kenya.

European Commission (2012). *Green Paper: Towards an integrated European market for card, internet and m-payments*. Brussels: EC.

Financial Action Task Force (FATF). (2014). *Guidance for a risk-based approach. The banking sector.* FATF/OECD. France.

Mobile Payments Industry Workgroup (MPIWG). (2012). *The US regulatory landscape for mobile payments*. Federal Reserve Bank of Atlanta and Federal Reserve Bank of Boston. Available at https://www.bostonfed.org/bankinfo/payment-strategies/publications/2012/us-regulatory-landscape-for-mobile-payments.pdf

Okuttah, M. (2012). *M-Pesa drives safaricom as profit declines to Sh12.8bn*, *Business Daily*. Available at http://www.businessdailyafrica.com/Corporate+News/MPesa+drives+Safaricom+as+profit+declines+/-/539550/1403606/-/35hl1b/-/index.html

Sultana, R. (2009). *Mobile banking: Overview of regulatory framework in emerging markets*. Bangladesh: Grameenphone Ltd.

Part III

The Challenges

7

Security Issues of New Innovative Payments and Their Regulatory Challenges

Safari Kasiyanto

Abstract Kasiyanto discusses how the security issues of m-payments and Bitcoin as new forms of innovative payments challenge the existing EU regulatory frameworks, and whether the proposed regulatory frameworks suffice to address such challenges. The regulatory frameworks Kasiyanto discusses mainly focus on the EU Payment Services Directive and the proposed changes of the directive. To some extent, it also touches upon the proposed directive on network and information security. Firstly, security issues of both systems are scrutinized to highlight their vulnerabilities. Secondly, the existing regulatory frameworks are assessed as to whether they suffice to address the challenges brought by the security vulnerabilities of both systems. Lastly, a final assessment is conducted to seek whether the proposed changes to the frameworks are adequate to address such challenges.

S. Kasiyanto (✉)
Ph.D. researcher, Tilburg Law and Economic Centre, Junior research fellow, European Banking Centre, Tilburg University, the Netherlands

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_7

Introduction

Innovative payments are one of the emerging markets in retail payments that potentially offer a huge benefit to the economy.[1] However, the adoption of most innovative payments is rather slow.[2] On the one hand, security and consumer perceived security play a significant role in the adoption of new innovative payments.[3] On the other hand, accessibility or usability of new innovative payments is also crucial.[4] While a consumer will never use a system that he or she perceives as unsecured, rigid security will possibly hamper the accessibility or usability of the method.[5] This condition has given rise to regulatory challenges as to how and to what extent the authority should regulate new innovative payments that keep the balance between security and accessibility of the payment methods.[6] In the EU for instance, the existing regulatory frameworks[7] have less deal with these issues and therefore, a new proposal has been introduced.[8]

This chapter tries to shed a light on the regulatory challenges exposed by the security issues of new innovative payments such as mobile payments (m-payments) and Bitcoin. Focusing on the EU regulatory framework, this study seeks the answers to the following questions:

---

[1] Innovative payments are part of electronic payments that, according to Moody's analysis, contribute to the increase of GDP by 0.8 % for developing countries and 0.3 % for developed countries. See details in Moody's: Moody's Analytics: The Impact of Electronic Payments on Economic Growth (2013). https://usa.visa.com/dam/VCOM/download/corporate/media/moodys-economy-white-paper-feb-2013.pdf.

[2] See for instance Key Pousttchi and Dietmar G. Wiedemann, "What Influences Consumers' Intention to Use Mobile Payments", *Mobile Communications Working Group*, *University of Augsburg* (2007) http://www.marshall.usc.edu/assets/025/7534.pdf.

[3] Changsu Kim, Wang Tao, Namchul Shin, and Ki-Soo Kim, "An empirical study of customers' perceptions of security and trust in e-payment systems", *Electronic Commerce Research and Applications* 9, no. 1 (2010): 84–95.

[4] See for instance Visa Europe Risk Management, "Secure Mobile Payment Systems, Recommendations for Building, Managing and Deploying", Visa Europe (2014). http://www.tuxedomoneysolutions.com/insights/research/2014/07/secure-mobile-payments/.

[5] See International Finance Corporation (IFC), "Mobile Money Study: Summary Report", 2011, Washington DC.

[6] Visa Europe Risk Management, "Secure Mobile Payment Systems", 5.

[7] In this context, Payment Services Directive (PSD): OJ L 319/1, 5 December 2007.

[8] Proposal for the revision of the Payment Services Directive (proposal for the PSD2), 24 July 2013 COM (2013) 547 final.

– How do the security issues of new innovative payments such as m-payments and Bitcoin give rise to the need for strengthening the existing regulatory frameworks?
– Does the proposed regulatory framework on payment systems suffice to address the security issues brought by m-payments and Bitcoin?

It is worth noting that the regulatory challenges arisen by security risks of m-payments and Bitcoin discussed here are limited to the challenges to the confidentiality, integrity and availability of the systems to process transactions. Confidentiality has the meaning that the transaction information is safe against unauthorized access, while integrity ensures that the transaction information will be intact while being processed and cannot be altered. Availability provides functionality of the systems that ensure the services are accessible and usable.[9] In other words, the challenges to protect consumer transactions and data against "conventional" crimes such as fraud, theft or hacking. Hence, challenges brought by payment system risks other than security risks such as liquidity and credit risks and newer challenges brought by more modern crimes such as money laundering and terrorism financing fall beyond the scope of this study.[10] However, although this study focuses on the objective security, as allocating liability for losses resulting from fraud and security breaches, in practice always done through legal and administrative processes rather than technological means,[11] this chapter will analyse not only legal provisions regarding the security requirements but also legal arrangements available for consumers to seek redress/remedy and consumer protection adequacy in general under the existing and proposed frameworks.

[9] Catherine Linck, Key Pousttchi, and Dietmar Georg Wiedemann, "Security Issues in Mobile Payment from the Customer Viewpoint" (2006). https://mpra.ub.uni-muenchen.de/2923/1/.

[10] For this, the World Bank provides an excellent elaboration. See Pierre-Laurent Chatain, "Integrity in Mobile Phone Financial Services, Measures for Mitigating Risks from Money Laundering and Terrorist Financing", *The World Bank Working Paper* No. 146. Washington DC (2008).

[11] See for instance Amir Herzberg, "Payments and Banking with Mobile Personal Devices", *Communications of the ACM* 46, no. 5 (2003): 53–58.

M-payments are the perfect example of a new innovative payment with slow and cumbersome adoption in more developed economies[12] whereas for Bitcoin, while its system is proven to be scientifically sound, the supporting systems such as a user's personal computer or exchange system are vulnerable from attacks.[13] In addition, both m-payments and the Bitcoin system represent the two most important factors after instant payments that trigger the next wave of innovation in the European markets, accounted for 28 % and 9 % respectively, based on the European Payment Council polling in 2015.[14] As for discussion on the regulatory frameworks, this study mainly focuses on the EU Payment Services Directive (PSD) and the proposed revisions of such a directive. However, elaboration on the proposed directive on network and information security will be also provided.

This chapter is organized as follows. Section "Some Insights on the Security Issues of New Innovative Payments" provides some insight on the security issues brought by m-payments and the Bitcoin system as the new forms of innovative payments. In particular, it highlights the new security risks of m-payments and the vulnerability of the supporting systems of Bitcoin. It is then followed by analysis on how these security issues give rise to the regulatory challenges: m-payments, the need for a more proper regulation and Bitcoin, whether merely a warning is adequate from the perspective of consumer protection. This analysis focuses on the existing regulatory framework, which is PSD,[15] and is provided in section "How Security Issues of New Innovative Payments Challenge the Existing Regulatory Frameworks". Analysis on the proposed regulatory frameworks including the way forward is provided in section "Do the Proposed Regulatory Frameworks Suffice? Elaboration on the Proposal of the PSD2, and the Way Forward". This chapter ends by conclusion in section "Conclusion".

[12] Niina Mallat, "Exploring Consumer Adoption of Mobile Payments – A qualitative Study", *Journal of Strategic Information Systems* 16 (2007): 413–432.

[13] Safari Kasiyanto, "Moving Forward, Bringing Bitcoin into the Mainstream" (Forthcoming).

[14] European Payment Council. Summer Reading: Results of Latest EPC Poll Reveal that Instant Payments are Most Likely Trigger the Next Wave of Innovation (blog). 7 August 2015.

[15] OJ L 319/1, 5 December 2007.

Some Insights on the Security Issues of New Innovative Payments

M-Payments and New Security Risks

M-payments covered by this chapter encompass three types: contactless, app-based and mobile network operator (MNO) channel payments.[16] The first is also known as proximity payments, while the last two fall under remote payments.[17] With proximity systems both payer and payee conduct the transaction from the same location using technologies such as infrared, Bluetooth or near field communications (NFC), while with remote systems the payer and payee conduct the transaction over networks, either a telecommunication network such as Global System for Mobile (GSM) communication or the internet.[18]

In every type of m-payment mobile devices serve as a double-edged tool,[19] meaning that such devices are used as a communication tool as well as a payment platform to initiate transactions with real money. As a result, new security risks have emerged.[20] These new security risks consist of the accumulation of the security risks embedded to mobile devices[21] and the security risks of the payment platforms used. Both risks are discussed in detail below.

---

[16] European Central Bank. "Recommendations for the Security of Mobile Payments, Draft Document for Public Consultations" (2013). https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf?7f9004f1cbbec932447c1db2c84fc4e9.

[17] Under the same group as the internet payments.

[18] See European Payments Council. "Overview Mobile Payments Initiatives." EPC091-14. Version 2.0. 2014.

[19] On the one hand, a mobile phone has functions for communication, and on the other hand it serves as a payment device to initiate transactions. See for instance Information Systems Audit and Control Association (ISACA). "Mobile Payments: Risk, Security and Assurance Issues." *An ISACA Emerging Technology White Paper*. November 2011. http://www.isaca.org/groups/professional-english/pci-compliance/groupdocuments/mobilepaymentswp.pdf.

[20] As highlighted by ECB, Recommendations for Mobile Payments.

[21] See for instance Vanessa Pegueros. "Security of Mobile Banking and Payments." *SANS Institute InfoSec Reading Room* (2012). https://www.sans.org/reading-room/whitepapers/ecommerce/security-mobile-banking-payments-34062.

Security Risks of Mobile Devices

A mobile device exposes relatively high security risks for payments as it is by nature made for a telecommunication portable device and not for a payment platform. The risks embedded in a mobile device vary from its design which makes it easier to be lost or stolen to limited input capability and malware.[22] In detail, such risks are the following.

The first risk is that a mobile device is designed as a portable tool, so it is easier to get lost or stolen. Data from consumerreports.org shows that in 2013 approximately 3.1 million mobile phones were stolen in the USA alone. It was nearly double from mobile phone thefts in 2012 which accounted for 1.6 million.[23] Out of 3.1 million stolen mobile phones, around 1.4 million were not recovered. Similar to this, another report by Lookout, Inc., a cybersecurity company with focus on mobile devices,[24] shows that in 2014 one in every ten persons who owns a smartphone is a victim of theft. The majority of these victims, approximately 68 %, are not successful in recovering their mobile phones.[25] As mobile phones contain so much personal data, according to the same report, 50 % of victims are willing to pay relatively high amounts of money (as much as USD500) to retrieve their precious data back such as photos, apps, videos, and personal information including that used for payments.

The second risk deals with the fact that mobile devices have inherently a limited input capability that is mostly triggered by the mobile device's physical factors. The limitations include size constraints, limited sensory capabilities up to 40 binary state buttons and form factors such as a standard keypad layout that places it awkwardly compared to QWERTY lay out. As a result, input using mobile devices is also limited as it is more problematic from a user's point of view and slower compared to larger

[22] Ibid, 12–14.

[23] Consumerreports.org. "3.1 Million Smart Phones Were Stolen In 2013, Nearly Double the Year Before." http://pressroom.consumerreports.org/pressroom/2014/04/my-entry-1.html. 17 April 2014.

[24] See https://www.lookout.com/. Last accessed on 29 November 2015.

[25] See Lookout, Inc. "Phone Theft in America." https://www.lookout.com/resources/reports/phone-theft-in-america. Last accessed on 29 November 2015.

devices such as personal computers.[26] Researchers keep trying to overcome these risks by expanding the mobile input, yet little progress has been made as the risks come from the nature of mobile devices as a portable device.

The third risk concerns the fact that a user of mobile devices has no control over the security configuration of his or her mobile devices on the one hand, while it is also difficult to protect the mobile devices against a malicious user on the other hand. The former is caused by the use of untrusted sources including untrusted mobile devices, networks, apps and contents,[27] while the latter is due to the fact that the user, even the malicious one, has full possession and therefore control in operating his or her mobile device. Trend.

The last risk deals with the malware of mobile devices that is rising fast. According to a report by Alcatel-Lucent,[28] approximately 16 million mobile phones worldwide were attacked by malware in 2014.[29] One notable security developer, McAfee, reports that until currently there have been more than 1,200 malware variants for mobile devices.[30] Malware attacking a specific Operating System (OS) of smartphones such as Android has also grown fast, such that in a few months last year it grew by 76 %.

Security Risks of the Payment Platform

Payment platform risks in m-payments include weak cryptography, in particular used by NFC systems, fraudulent transactions, attacks to Subscriber Identity Module (SIM) card application (Unstructured

[26] Edward C. Clarkson, Shwetak N. Patel, Jeffrey S. Pierce, and Gregory D. Abowd, "Exploring Continuous Pressure Input for Mobile Phones" (2006) ftp://coffeetalk.cc.gatech.edu/pub/gvu/tr/2006/06-20.pdf.

[27] Murugiah Souppaya and Karen Scarfone, "Guidelines for Managing the Security of Mobile Devices in the Enterprise", *NIST Special Publication* 800, (2013):124.

[28] https://www.alcatel-lucent.com/about. Last accessed on 29 November 2015.

[29] See Leon Spencer, "16 Million Mobile Devices Hit by Malware in 2014: Alcatel-Lucent", Available at http://www.zdnet.com/article/16-million-mobile-devices-hit-by-malware-in-2014-alcatel-lucent/.

[30] http://home.mcafee.com/advicecenter/?id=ad_ms_wimm&ctst=1. Last accessed on 29 November 2015.

Supplementary Service Data (USSD) or Dynamic SIM ToolKit (DSTK)), threats on mobile application server and database, and native application security of m-payments.[31] The complexity of these security risks is worsened by the fact that from the demand side, most consumers of m-payments have a lack of awareness of the security issues whereas from the supply side, more and more services are provided by third-party providers that have, by nature, less or no expertise on the security and security issues of payment systems.[32]

If not well mitigated, these risks may have impact on not only the business revenue losses resulting from the fraudulent transactions but also privacy and confidentiality breach and communication service misuse.[33] Securing m-payments requires a combined expertise between technical security of payment platforms and that of mobile devices. This includes securing data storage on the mobile device, securing data transmission from mobile device to app server and vice versa, implementing strong authentication in particular for app-based m-payments, securing web interfaces and services for web-based m-payments and validating the trusted and untrusted inputs for app-based.[34]

Bitcoin and the Vulnerability of Its Supporting Systems

As Fred Wilson wrote: "One of the real issues with Bitcoin right now is that it's not that secure, and the reason it's not that secure is, it's easy to hack into people's computers, if they have a wallet on their own computer, it's easy to get in there and steal the Bitcoin (…).".[35]

---

[31] Suhas Desai, "Mobile Payment Services: Security Risks, Trends and Countermeasures", RSA Conference 2014. Asia Pacific & Japan (2014) http://www.rsaconference.com/events/ap14/agenda/sessions/1447/mobile-payment-services-security-risks-trends-and.

[32] ECB, Recommendations for Mobile Payments, November 2013. https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf?7f9004f1cbbec932447c1db2c84fc4e9.

[33] Desai, Mobile Payment Services, p. 8.

[34] See Ibid, 21.

[35] Rob Wile, "One of Bitcoin's Strongest Backers Reveals the Two Big Reasons Why It's Still Not Mainstream." 20 July 2014. http://www.businessinsider.com/fred-wilson-on-bitcoin-2014-7?IR=T.

Wilson is a Bitcoin proponent who has invested a lot of money in the Bitcoin system since its beginning. He pointed out the security issues of Bitcoin that lie with the vulnerabilities of the supporting systems such as a user's wallet. Furthermore, he believes that as a virtual currency Bitcoin needs to be more secure if it wants to be widely adopted as a mainstream payment.[36] Using Wilson's opinion on Bitcoin security issues as a starting point, this section briefly explores the security issues of Bitcoin.

The security issues surrounding the Bitcoin system vary, from the (minor) vulnerabilities of the system to the attacks to both users and exchanges to viruses and malware. However, the most successful attacks to steal Bitcoin came from outside the peer-to-peer system such as the user taking less precaution in keeping his or her electronic wallet safe or the attacks to the exchange system. The peer-to-peer system itself has been proven to be scientifically sound.[37] For this reason, it is justified to claim that the vulnerability of the Bitcoin systems lies with "supporting" systems[38] used by the participants, such as those of users and exchanges, rather than the peer-to-peer system itself. However, both security issues will be briefly discussed below.

Security Issues of the Peer-to-Peer System

The latest security issues of the peer-to-peer system include double-spending attack, 51 % hash power attack and minor vulnerability. The first issue, the double-spending attack is possible by forcing a forged blockchain in a bogus (second) transaction.[39] This risk has actually been recognizable since the beginning.[40] It can be done by altering the first transaction and publishing the altered transactions into the network for authorization. If the user connected to large numbers of miners, the

[36] Ibid.

[37] Kasiyanto, Moving Forward.

[38] Jeff Desjardins, "How Secure are Bitcoins?", Visual Capitalist. www.visualcapitalist.com/secure-bitcoins/ 13 August 2014.

[39] Meni Rosenfeld, "Analysis of hash-rate-based double-spending", Latest version: 13 December 2012. https://bitcoil.co.il/Doublespend.pdf.

[40] See Satoshi Nakamoto, "Bitcoin: A peer-to-peer Electronic Cash System", Consulted 1.2012 (2008).

altered transaction might be proven early and placed as a blockchain, while the first transaction remains processed, forgotten or even rejected. To some extent, the method used in double spending is similar to that of transaction malleability,[41] only the subject is different. However, this fraud is much more applicable in theory but difficult in reality for several reasons. First, the user needs to be adept in transactions using Bitcoin and the blockchain. Second, he or she needs to be exposed to a large number of miners' networks. And last, there is no economic incentive to do so from the network's point of view. The last has the meaning that in order to prove transactions a miner alone needs a superpower computer, and he or she will be more benefitted to complete an authorized transaction and to be rewarded with Bitcoin rather than involve in a bogus transaction.[42]

The 51 % hash power attack is possible considering that the Bitcoin system relies on peer-to-peer authentication. A player having 51 % power or more will be able to manipulate the system for their own advantages. It is related to the fact that to approve a transaction, the Bitcoin system depends on the network. Hence, a person having 51 % or more power of the network will be able to drive the transaction approval. That is why when GHash.IO was almost reaching 51 % power, the Bitcoin market was panicked.[43] However, the economic incentives of 51 % hash power attacks remain doubtful.

The last security issue concerns some minor vulnerabilities such as that in the Universal Plug and Play (UPnP) library used by Bitcoin Core.[44] A certain version of the *miniupnpc* library is vulnerable to a buffer overflow that might be used by fraudsters to crash the application by running a

[41] For a good discussion on this, see for instance Emin Gun Sirer. "What Did Not Happen at Mt. Gox." 1 March 2014. http://hackingdistributed.com/2014/03/01/what-did-not-happen-at-mtgox/.

[42] https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-security-of-transaction-block-chains, last accessed on 28 October 2015.

[43] Jonas Borchgrevink, "Warning: GHash.IO is Nearing 51 % – Leave the Pool", *Crypto Coins News*. 9 January, 2014. https://www.cryptocoinsnews.com/warning-ghash-io-nearing-51-leave-pool/.

[44] *Vulnerability in UPnP library used by Bitcoin Core*, 12 October 2015. https://bitcoin.org/en/alert/2015-10-12-upnp-vulnerability.

malicious server.[45] However, this can be easily prevented by, for instance, keeping the relevant software updated.

Security Issues of the Supporting System

The Bitcoin ecosystem consists of miners, exchanges, users and merchants. As Bitcoin is a cryptographic currency used for online transactions, each participant in the ecosystem needs a supporting system.[46] Miners need a set of computers enabling them to authenticate blockchain, exchanges need a system enabling users to exchange Bitcoin with real money, users need an application to create a wallet and restore Bitcoin, while merchants need a system enabling them to accept Bitcoin as a means of payment. If we have blockchain in Bitcoin transaction, here we have a "system-chain" where each system within the ecosystem is connected to each other to support the transactions using Bitcoin. The rule of a chain is that it is only as strong as its weakest link,[47] and some of the supporting systems are vulnerable, such as those of users and of exchanges.

Security issues include attacks to users resulting in one in every 16 or 17 Bitcoin belonging to whoever has stolen it. Since 2009 over USD500 million worth of Bitcoins have been stolen.[48] It seems that any parties involved in the Bitcoin system are aware of this vulnerability. For instance, online warning and guidance on securing your Bitcoin wallet include advice on taking precautionary steps such as to back up your user's wallet (back up the entire wallet, make regular backups, encrypt the online backups and use many secure locations for backups), use a strong password

[45] TALOS Vulnerability Report. "MiniUPNP Internet Gateway Device Protocol XML Parser Buffer Overflow." TALOS-2015-0035. 15 September 2015. http://talosintel.com/reports/TALOS-2015-0035/

[46] The term of "supporting system" does not need to be interpreted literally. It is a general term used to make the analysis easier.

[47] "In every chain of reasoning, the evidence of the last conclusion can be no greater than that of the weakest link of the chain, whatever may be the strength of the rest." Reid, Thomas. *Essays on the Intellectual Powers of Man* (1786) as in http://www.phrases.org.uk/meanings/the-weakest-link.html.

[48] Desjardins, How Secure are Bitcoins?, on 13 August 2014, http://www.visualcapitalist.com/secure-bitcoins/.

and never forget it, keep updating the software and use multi-signature for protection against theft.[49] Below is an example of warnings before a user wishes to use Bitcoin (from https://bitcoin.org). The similar warnings can be easily found on the webs providing services using Bitcoin: "(…) Many exchanges and online wallets suffered from security breaches in the past and such services generally still do not provide enough insurance and security to be used to store money like a bank… Additionally, using two-factor authentication is recommended".[50]

Another big security issue deals with the exchange systems. Up to recently there were 12 attacks to exchange systems including the most phenomenon attack which was to Mt. Gox. In February, Mt. Gox was reported filing for bankruptcy after approximately 850,000 Bitcoins (among which 750,000 Bitcoins belong to customers), worth nearly USD500 million, were stolen due to security breaches. Later on this year, the former founder and CEO of Mt. Gox was reported as having been arrested in Japan and questioned regarding the disappearance of the virtual currency.[51] So many scenarios spread all over the internet about what exactly went wrong with Mt. Gox system. Some suggest that "transaction malleability" has caused such tragic losses, while others suggest that Bitcoin keypersons have lost their private key to access the cold storage. Some others even suggest hackers succeeded in intercepting the exchange system and taking away hundreds of thousands of Bitcoin.[52] Beside all these scenarios, the fact that hundreds or thousands of customers have lost their Bitcoin is an adequate evidence that the exchange system is vulnerable.

[49] https://bitcoin.org.

[50] *Securing your wallet*, *Be careful with online services*. https://bitcoin.org/en/secure-your-wallet. Last accessed on 28 October 2015.

[51] http://www.theguardian.com/technology/2015/aug/01/ex-boss-of-mtgox-bitcoin-exchange-arrested-in-japan-over-lost-480m. Last accessed on 30 November 2015.

[52] For an insight, see Sirer, What Did Not Happen. See also https://winklevosscapital.com/what-may-have-happened-at-mt-gox/, http://www.hackingdaily.com/2014/02/mtgox-speculations.html, and https://www.reddit.com/r/Bitcoin/comments/1z8fmc/mtgox_private_key_related_coin_loss_a_explanation/. Last accessed on 30 November 2015.

How Security Issues of New Innovative Payments Challenge the Existing Regulatory Frameworks

Within the EU, secure and safe payment systems are the required condition for the payment market to be well functioning to support market integration.[53] Therefore, in order to support EU market integration, it is compulsory for innovative payments such as m-payments and the Bitcoin system[54] to be secure and safe. However, as previously discussed, both m-payments and the Bitcoin system expose relatively different security risks: m-payments with new security risks and the Bitcoin system with the vulnerabilities of its supporting systems. This section discusses how these different security risks challenge the existing EU regulatory frameworks.

M-Payments: The Need for a More Proper Regulation

Security issues of m-payments that give rise to regulatory challenge consist of several factors involving the adequacy of not only the technical factor but also the legal factor. The technical factor encompasses the adequacy of the security level that, on the one hand, provides high-level protection and, on the other hand, encourages the usability of the payment method. The legal factor lies in particular on a basic framework for consumer protection, consisting of a redress arrangement enabling consumers to seek remedies and limited liability for consumers. This comes from the fact that disputes arising from technical factors such as security issues will be solved using administrative and legal instruments.

[53] Proposal for PSD2, paragraph 6 of the preamble, 14.

[54] Here Bitcoin is treated as a payment system instrument. For discussion as to whether Bitcoin meets the characteristics and requirements of payment instruments, see Safari Kasiyanto, "Regulating Peer-to-peer Network Currency: Lessons from Napster and Payment Systems", *Journal of Law, Technology and Public Policy* 1(2) (2015): 40–73.

Adequate Security that Encourages the Usability of the System as Basic Requirement

Adequate protection of consumers against risks exposed by security issues is crucial in payment systems.[55] However, as high-level security requires a lot of investment on the one hand, and as the usability of a payment system is also crucial to ensure the sustainability of the system on the other hand, security measures taken by the providers of m-payments have to be proportionate to the security issues concerned.[56] Hence, regulation on the security measures needs to keep the balance between maintaining an adequate security level and encouraging the usability of the systems.

Regulation imposing the security measures must also be timely and technologically neutral. As the security methods are dynamically evolved to keep up with the evolving threats—what considered secure today may not be safe tomorrow—regulation that does not easily become obsolete is the most favourable. In addition, technological neutral regulation is also encouraged. To answer these challenges, the possible solution is a regulation that imposes general principles for security yet which are clear and strong enough to protect consumers. In this manner, the general principles ensure that adequate protection to the consumers takes place while the usability of the systems is promoted. A general principle regulation also guarantees the timely objective and neutrality of the legislation. To fill in the gaps between the general principles and detailed security needed in implementation, such a regulation must be accompanied by a standard containing the technical details of the security. This standard would be best drafted and agreed by market players rather than imposed by a regulator as business interests also play a crucial role in defining the standard. For instance, interoperability of two m-payment systems deals with not only opening and sharing each other's technical securities and specifications, but also willingness to share with each other the business platform. The existing regulatory framework will firstly be analysed against this basic requirement.

[55] Proposal for PSD2, paragraph 6 of the preamble, 14.

[56] Proposal for PSD2, paragraph 7 of preamble, 15.

Security Requirements Under the Existing Regulatory Framework

Under the existing regulatory framework in the EU, the general principles regarding the security of the payment systems are regulated under article 57 of the PSD, ruling that payment service providers are obliged to ensure that the personalized security features of the payment instrument are not accessible to other parties. Hence, the obligation for payment providers to protect the consumer data against unauthorized accesses is explicitly stated by the law. The consequences of this provision if not satisfied by payment providers are laid down under article 60(1) of the PSD, in which the payment providers shall provide a refund immediately to the consumers of an amount equal to the amount of unauthorized transaction. In addition, article 60(2) of the PSD also makes it possible for consumers to seek any financial compensation if the contract concluded between the providers and consumers enables the consumers to do so.

Although the above mentioned general principles cover adequate rules for the security of payment systems in general, there are some difficulties in applying such rules to m-payment systems for several reasons. Firstly, m-payment providers not only vary—from banks to MNOs to app-based start-up companies—but also some of them are new players that are not yet covered by regulations. Regarding the new m-payment providers that are rising fast, the European Payments Council provides an insight that within five months alone, from June 2014 to October 2014 there were at least 19 new Single Euro Payments Area (SEPA) initiatives in the EU, from TouchGo used for vending machine transactions in UK to Telecom Italia for mobile point-of-sale (mPOS) transactions in Italy.[57] Furthermore, among these players are the so-called third-party payment service providers that basically provide payment services that link their own platform to the account servicing platforms using mobile applications. For consumers, using services provided by entities that are not yet covered by regulations exposes high risks.

Secondly, m-payment providers by nature have less or no expertise in dealing with the security and the security issues of payment systems.

[57] EPC, Overview Mobile Payments Initiatives, 21, 25.

This in particular applies to the start-up companies providing app-based payment services. Although for MNOs, dealing with security issues of payment systems requires different expertise as they differ from those of telecommunication systems. Payment systems involve converting real money into "electronic" money (and vice versa in case of redeeming[58]) that can be used for purchasing goods or services in many (online) places or performing any other online transactions (such as person-to-person online transfers), while telecommunication services deal with a narrower activity, communication in distance. Considering this circumstance, and observing that m-payments have brought new risks, the existing regulatory framework must be strengthened in order to protect the consumers that in the end also ensure the sustainability of the systems.

Other obligations imposed under the PSD to the payment providers are to provide evidence of payment transactions in case of any disputes and, when necessary, to process personal data in order to safeguard the prevention and detection of payment fraud (under article 79 of the PSD).[59] The former obligation is quite clear and must also be applied to m-payment providers, while the latter must be applied in accordance with Directive 95/46/EC on Data Protection. This directive is now also under review for major revisions.

As the obligation on the security measures under the PSD is, on the one hand, too broad and varied, while the m-payment providers, on the other hand, consist of different players, there is a need for clarity in terms of detailed security requirements or common standards. However, these common standards are currently not in existence. As a result, different service providers employ different security for the same services: m-payments.

Sufficient Consumer Protection Provisions

Sufficient consumer protection encompasses at least two aspects of protection: redress arrangement enabling consumers seeking remedies and

[58] Converting back the 'electronic' money into the real currency.

[59] Chapter 4 of the PSD on Data Protection.

limited liability for consumers. Below is the discussion of these aspects under the existing frameworks.

Firstly, the redress provisions for consumers seeking remedies are regulated under article 60(1) and 60(2) of the PSD. As previously touched upon, the rules generally oblige the payment providers to provide a refund immediately for any unauthorized transactions (under article 60(1)) and allow the consumer to seek any additional compensations provided that the contract enables consumers to do so (under article 60(2)). This provision is basically adequate as it strongly obliges the service providers to compensate the consumers for any unauthorized transactions. However, challenges arise in applying this framework to m-payments. First, it would be difficult for consumers of certain m-payments such as those using NFC technology or MNO channels to prove unauthorized transactions. For instance, if a consumer loses his or her mobile device which he or she used for m-payment services through NFC or MNO channels, it will be much easier for the thief to perform any "authorized transactions" using such a device as all necessary sensitive information for authentication may be accessible. Second, as some of the payment providers, in particular the third-party payment service providers, are not yet brought under the existing regulatory frameworks or designated under the oversight of the authority, it will be difficult to apply article 60 of the PSD to them. As a result, it would be difficult for consumers to seek compensation for any unauthorized transactions.

Secondly, the limited liability framework for consumers is mainly regulated under article 56 of the PSD. Such a framework includes zero liability for the consumer after notification of any lost or stolen instruments, limited liability up to a maximum of EUR150 if the consumer fails to keep the instruments safe, and full liability if the consumer involves in fraud or acts of gross negligence. When applying this liability framework to m-payment consumers, challenges arise.

The first challenge deals with the underlying mind-set of the liability framework, which is based on lost or stolen instruments. Consumers will be released from any liability (equal to zero liability) once they have notified the service providers of any lost or stolen instrument. In contrast, consumers will be held liable (up to a maximum amount) if they neglect to do so. The challenge is that m-payments are conducted

through mobile devices, and a mobile device is not a payment instrument such as a credit card or debit card. The main function of mobile devices remains as a communication tool. It is impractical for consumers to notify m-payment providers of any lost or stolen devices. For instance, in the case of MNO based m-payments, theoretically it will take several attempts for consumers to make notification to m-payment providers. The longer the time between such loss and notification will give more opportunity for the thief to get financial gain by performing unauthorized transactions. This in particular applies to some m-payments using NFC technology and MNO channels.

The second challenge deals with the maximum amount of the consumer's liability which is EUR150. M-payments are mainly used for micropayments involving a small monetary value, individual and day-to-day transactions such as buying a cup of coffee or person-to-person transfers (mostly without any underlying transaction). The Mobile Payments Index provided by Ayden[60] shows that the average transaction value of online purchases made using mobile devices in 2014 amounted to "only" EUR28.27. Although it increased by 37 % from the transactions in 2013 (approximately at EUR20.6), it is still very low compared to the maximum amount of liability. Hence, the limited liability for consumers at a maximum of EUR150 is indeed too high.

Bitcoin from the Perspective of Consumer Protection: Why Merely a Warning Is Not Adequate

Like that of m-payments, the usability of Bitcoin is also hampered by the security issues.[61] Particular security issues that might give rise to regulatory challenge consist of two parts. Firstly, it deals with the fact that as a new payment method that totally differs to the existing payment systems, the Bitcoin system is not yet covered by regulation. Secondly, although

[60] See Ayden, "Over 27 % of global online transactions are now on mobile devices", 30 April 2015. Available at https://www.adyen.com/home/about-adyen/press-releases/mobile-payments-index-april-2015. Last accessed on 17 November 2015.

[61] Wile, One of Bitcoin's Strongest Backers Reveals.

the Bitcoin system claimed to be the most secure system technically, lost or stolen Bitcoins and breaches at exchanges keep occurring.

New Payment Method Not Covered by Regulation

As discussed in the previous chapters, the possible approaches in dealing with the Bitcoin system are to regulate, to ban, or to stay with the status quo. So far, no single jurisdiction explicitly bans Bitcoin, but some give warnings. The latter includes China, EU and France, emphasising that consumers who use Bitcoin are exposed to some risks as the system is not yet covered by the existing regulations. Hence, consumers need to take all necessary precautionary steps to mitigate the risks.

The existing regulatory frameworks in the EU also say nothing about the peer-to-peer system. The most relevant regulatory frameworks are the PSD and the directive on e-money,[62] yet Bitcoin falls beyond the scope of both frameworks.[63]

The question is now whether it is necessary to bring the Bitcoin system under the regulatory frameworks. If yes or no, under what grounds. Considering that the Bitcoin market is still relatively small, perhaps it is not yet necessary to regulate Bitcoin. However, considering that the supporting systems are vulnerable as lost/stolen Bitcoin keeps occurring, there is a need to strengthen the consumer protection, in particular to prevent such lost/stolen Bitcoin from happening again in the future. As creating any remedy arrangements is nearly impossible due to the fact that transactions using Bitcoin are, by systems, irreversible and irrevocable, the preventive actions are the only available option.

The next question is how to strengthen the consumer protection if the solution to bring the Bitcoin system under regulatory framework is not yet an option. What measure is available to strengthen the consumer protection besides regulation? These questions raise regulatory challenges

[62] Directive 2009/110/EC, OJ L 267/7. 10 October 2009.

[63] See European Central Bank, "Virtual Currency Schemes", 2012. In this report, ECB eloquently elaborates the rise of virtual currencies and uses Bitcoin as one of the case studies. It concludes that the peer-to-peer crypto system falls beyond directive on e-money and the PSD.

in the broader scope. As regulation is not yet an option, regulatory frameworks in a wider meaning could apply. By wider it has the meaning of soft laws. These could include a guideline from the authority or a code of conduct or bye-laws among the market players.

After assessing the circumstance, now it is much easier to understand why over 30 jurisdictions including China, the EU (in this case the European Banking Authority), the USA and many others issued warnings, to alert the consumers of the risks of using Bitcoin as it is not yet covered by the existing regulatory frameworks. In the most ideal condition, merely warnings are not sufficient to protect consumers. However, considering the difficulties arising from the nature of the peer-to-peer transactions, and that the aggregate volume of transactions is still relatively insignificant, it is now much easier to understand why no regulation has been adopted, and only warnings are issued.

Said the Most Secure, But Lost/Stolen and Breaches Keep Occurring

Although the peer-to-peer system of Bitcoin has proven to be scientifically sound, lost/stolen Bitcoin keeps occurring resulting in USD500 million worth of Bitcoin stolen over the last five years. It means that one in every 16 or 17 Bitcoins in circulation today belongs to someone who has stolen it. Who is to blame? The vacuum of any regulations to protect consumers, Bitcoin community that has not yet matured in creating adequate code of conducts, or reckless users? In addition, 12 exchanges were also attacked my fraudsters resulting in the loss of millions of Bitcoin worth hundreds of millions USD. As a result, many governments issued warnings about risks embedded in using Bitcoin that consumers must be aware of. Do such warnings mean anything or have any implications to the Bitcoin theft?

Before discussing the warnings, the possible attacks to exchange systems will be discussed to point out that decent consumers have been the victims, ending up with losing in total hundreds of millions of Bitcoin. The first possible attack is transaction malleability. Basically, the attacker node alters the transaction and broadcasts the altered transaction into the

network for authorization. For illustration,[64] suppose that the original transaction says "Alice is a great student". The attacker then changes it, in a non-substantial meaning or validity, into "Alice is a good student", and then publishes this altered transaction. Although different, both the original and the altered transaction are true. Unfortunately, what matters in the Bitcoin transaction system is what is true or not true. Once the altered transaction becomes prevalent, the miners will approve it and put it into the next blockchain. The original transaction will be forgotten and rejected. If this transaction malleability is repeatedly conducted to withdraw real money at the exchanges, over and over again in huge amounts, it will significantly harm the exchange and decent customers who use such an exchange. Ken Shirriff provides a chart that on 10 and 11 February 2014, up to 25 % transactions (accounting for nearly 1,000 transactions) in the Bitcoin system were observed using the transaction malleability.[65] The second possible issue is that exchanges employ low-level management and have poorly designed and poorly accessible cold storage. The former makes it easier for a hacker to attack, including a "janitor attack" which slips in with a universal serial bus (USB) and installs malware into the exchange system's PC, while the latter is more poor management that makes the cold storage no longer accessible for a more ridiculous reason, such as misplacing the private key. The fact is that exchanges are mostly start-up companies that are very rare to invest high amounts of capital and resource on security. The last possible attack is carried out by an insider as a result of weak control and management. However, whatever the reasons it leaves decent consumers unprotected and becoming the victims.

Unfortunately, a warning is not a legal instrument, nor is it a legislative product or regulation. It aims at providing information for consumers, so they would be more cautious about the product and the risks embedded, and further encourages consumers to take all necessary steps to mitigate the risks. It is more an *ex ante* rather than *ex post* instrument.

---

[64] This illustration is generated from that of Cameron Winklevoss. "What May Have Happened at Mt.Gox." https://winklevosscapital.com/what-may-have-happened-at-mt-gox/. Last accessed on 30 November 2015.

[65] See Ken Shirriff. "The Bitcoin malleability attack graphed hour by hour." http://www.righto.com/2014/02/the-bitcoin-malleability-attack-hour-by.html. Last accessed on 30 November 2015.

The former has the meaning for prevention, whereas the latter can be used for remedy. In this manner, such a warning has no implication to address the Bitcoin thefts for it has neither the intention nor the goal to do so. As no single legal instrument is available to provide for regulatory frameworks for the Bitcoin system, in this case consumers will be left unprotected.

In further steps, these conditions have challenged the existing regulatory framework and measures adopted by government (which in this case are warnings) for ignoring the protection of decent consumers.

Do the Proposed Regulatory Frameworks Suffice? Elaboration on the Proposal of the PSD2 and the Way Forward

In general, the proposal for PSD2 maintains the existing regulatory frameworks relating to the security of payment systems, with several revisions to strengthen some weaknesses.

M-Payments Under the Proposal for Revision of the Payment Services Directive and Security Recommendation

Besides the proposal for PSD2 the EU regulator also proposed a recommendation for the security of m-payments.[66] Introduced on 20 November 2013 by the European Central Bank (ECB), the draft of recommendation was actually developed by the European Forum on the Security of Retail Payments (SecuRe Pay Forum[67]) with the objective of determining the

[66] ECB, Recommendations for Mobile Payments.

[67] A cooperation initiated between the relevant authorities in payment systems within the European Economic Area, established in 2011, with objectives of sharing, understanding and facilitating platforms regarding the security issues of electronic retail payment systems. If necessary, this forum may issue any recommendation on the subject matter. See ECB. "Mandate of the European Forum on the Security of Retail Payments." October 2014.

minimum requirements applied for m-payment systems.[68] Discussion in this section will also include a review of such a recommendation.

Security Regulation Under the Proposal of the PSD2

The proposal of the PSD2 maintains the general principles imposed under the PSD with slight changes. The provisions on the security measures are ruled under Chap. 5 on Operational and Security and Authentication, article 85 to 87, envisaging at least four different aspects: security requirements, incident notification, security assessment reporting and authentication (see Table 7.1).

The first provision deals with the security requirements. Under the proposed article 85(1) payment providers are obliged to employ security measures that are appropriate to the risks embedded. However, the provision as laid down under article 85(1) is made with reference to the proposed network and information security (NIS) directive, with special reference to provision on risk management (article 14).

The second provision concerns the incident notification that must be made by the payment providers to the designated authority, from designated authority to the competent authority of home Member State and EBA, and from EBA to the competent authorities of other Member States. Where the security incident has a significant impact on the financial interests of the users, payment providers are obliged without undue delay to notify the users.

The third provision regulates the payment provider's obligation to report to the designated authority regarding the assessment of the operational and security risks of their system, and how to mitigate and control them. Such reports must be updated on a regular basis. To provide a guideline on this, the proposed directive requires EBA in close cooperation with ECB to develop such a guideline and review it on a regular basis. If necessary, such a guideline may include the certification processes. In addition, EBA must also develop the guideline on the qualify-

[68] See EPC Newsletter. "EPC Comments on the Draft Recommendation for the Security of Mobile Payments Developed by the European Forum on Security of Retail Payments." 29 April 2014.

Table 7.1 Security regulation under the proposal of the PSD2

No.	Topics	Proposed rules	Article
1.	Security requirements	Refer to the proposed NIS directive, including obligation on risk management under article 14 of the proposed NIS directive	85 (1)
2.	Incident notification	Payment provider's obligation to notify any security incident refers to articles 14 and 15 of the proposed NIS directive Where the incident has a significant impact, payment providers are obliged to notify users Obligation of the competent authority to notify home Member State authority and European Banking Authority (EBA), and EBA to notify the competent authorities of other Member States	85(2)–(4)
3.	Security assessment reporting	Payment providers are obliged to report and update the competent authority regarding the assessment of the operational and security risks and how to mitigate and control them EBA cooperated with ECB to develop and review on regular basis guidelines on the security measures, including certification EBA also develops guideline on the qualifying security incidents to be reported	86(1)–(4)
4.	Authentication	Payment providers are obliged to apply strong authentication Exceptions may be made under EBA rules based on risks involved EBA shall issue guideline on this within two years after the adoption of the directive	87(1)–(3)

Source: The Proposal of the PSD2

ing security incidents to be reported to the authority as mandated under article 85(2)–(4).

Finally, the last provision deals with the authentication for consumer transactions. Payment providers are obliged to apply strong authentication processes for consumer transactions. However, exceptions to this rule may be made by EBA based on the risks involved on the payment systems used. Therefore, EBA shall issue a guideline on the authentication and its exemptions within two years after the adoption of the proposed PSD2.

Security Requirements Under the Proposed Recommendation

The proposed recommendation consists of five guiding principles and 14 implementing recommendations. The five guiding principles are that m-payment providers should:

- Identify, assess and mitigate the risks embedded with their services;
- Implement strong authentication mechanism;
- Protect customer's data both in transit and at rest;
- Employ secure management for authorization and monitoring transactions in order to prevent fraud; and
- Provide information on security issues to customer and engage in customer education.
- Those five guiding principles are broken down in detail under the 14 recommendations that consist of three areas: general control and security requirement, specific control and security measures applicable for m-payment and customer education and communication. In detail the 14 recommendations are very rigid due to the objective to achieve a high standard of security of m-payments. Such recommendations consist of the following:
- Recommendation 1 Governance.
- Recommendation 2 Risk assessment.
- Recommendation 3 Security incident monitoring and reporting.
- Recommendation 4 Risk control and mitigation.
- Recommendation 5 Traceability.
- Recommendation 6 Initial customer identification and information.
- Recommendation 7 Strong authentication.
- Recommendation 8 Provision of authentication tools and software.
- Recommendation 9 Authentication attempts and time-out.
- Recommendation 10 Transaction monitoring.
- Recommendation 11 Protection of sensitive and personal data.
- Recommendation 12 Customer education and communication.
- Recommendation 13 Notifications and setting of limits.
- Recommendation 14 Customer access to information on the payment status and execution.

Consumer Protection Provisions Under the Proposal of the PSD2

As previously explained, consumer protection provisions regarding security issues consist of two elements: redress arrangement and liability framework. Under the proposal of the PSD2, redress arrangement of an unauthorized transaction to a consumer is ruled under article 65. It generally maintains the provisions imposed under the PSD: the payment provider is to refund immediately to the consumer any unauthorized transactions, and additional financial compensation is possible in accordance with the law applicable to the contract between the payment provider and the consumer. Furthermore, liability framework for unauthorized transactions is ruled under article 66 that also maintains the provisions under the PSD, with a slight change regarding the maximum amount for an unauthorized transaction a user can pay that is reduced from EUR150 to EUR50.

Analysis of the Proposed Frameworks

With regard to the adequacy of the security, the overall arrangements under the proposal of the PSD2 accompanied by a detailed guideline on the common minimum security requirements under the recommendation from the SecuRe Pay Forum seems promising as there is a legislation imposing the general principles accompanied by a recommendation on the technical standards. Promising in terms of guaranteeing the high level of security on the one hand, and encouraging the usability of the system on the other hand.

However, if one takes a look into the details, the proposed arrangements have some ambiguities. On the one hand, the general principles maintained under the proposal of the PSD2 are too broad so it is not strong enough to ensure the adequacy of the security. The explicit wordings under the PSD that oblige the service providers to employ high-level security is actually erased from the proposal of the PSD2. Instead, it makes a reference to the obligation under the proposal of another directive, the directive on NIS, which is currently also under discussion. This gives rise to uncertainty as both proposed directives are now under discussion. There is no guarantee regarding which directive will be adopted first, or even a guarantee that the proposed NIS directive will be adopted. On the

other hand, if one looks at the details of the recommendations developed by SecuRe Pay Forum and introduced by ECB, the security requirements proposed in such recommendations are too rigid. Although in terms of ensuring a high level of security such rigid requirements are a better option, they may hinder the adoption of m-payments in the market. This challenge was in particular brought by the European Payment Council.[69] Currently in the EU, m-payments are at the very early stage of development. Imposing a more lenient framework that keeps the balance between security and usability of the systems is more desirable if one wishes to see m-payments flourish. The lesson learnt from flourishing m-payment schemes in developing countries, M-Pesa in Kenya for instance, is that m-payments tend to flourish under more lenient regulatory frameworks.[70]

The provision of sufficient consumer protection, as explained under the existing framework, consists of two elements, namely a redress arrangement enabling consumers to seek remedies and a limited liability framework for consumers. Under the proposed framework, both revisions are maintained with a proposed change only on the maximum amount of the liability borne by consumers from up to EUR150 to EUR50. Considering that m-payments are used for micropayments—low value (the average value per transaction amounted to EUR28.27 in 2014), individual and daily transactions—the proposed reduced amount is a good progress and therefore needs to be supported.

The Proposed Directive on Network and Information Security (NIS) to Cater for Bitcoin Supporting Systems: Proposal to Regulate Bitcoin Exchange

Bitcoin Under the Proposal of the PSD2

The proposed framework, the proposal of the PSD2, remains silent with regard to Bitcoin activities. Based on the scope and definition under article 1 of the proposal, the directive will maintain the limited application to the following entities: (i) credit institutions, including banks, (ii) electronic

[69] Ibid.

[70] See IFC, Mobile Money Report.

money institutions,[71] (iii) post office institutions, and (iv) payment institutions.[72] As a peer-to-peer network currency and decentralized system, the Bitcoin system is totally different to any of the existing payment systems. Although it is possible to treat Bitcoin as a payment instrument, it is impossible to identify who is the "service provider" in the Bitcoin system as the supply of Bitcoin is determined by the system, and the transaction is authenticated by miners by discovering the new blockchain. Hence, the proposal of the PSD2 still cannot be applied to the Bitcoin system.

Bitcoin Under the Proposed NIS Directive

However, the proposed NIS directive[73] might be applicable to the Bitcoin system. Under this proposed directive, the "NIS" term has a broader meaning since it may include the Bitcoin system under the following provision:

> (…) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted… for the purpose of their operation, use, protection and maintenance (emphasis given).[74]

As Bitcoin is basically computer data protected by a sophisticated algorithm that can be stored, processed and transmitted via computer networks, the proposed NIS directive may apply. This proposed directive serves as a legal framework to ensure a high level of security applied to both network and information systems.[75] The most significant provisions on the security issues under the proposed NIS directive are laid down in article 14, ruling that service providers (the directive uses the term

[71] Under directive 2009/110/EC on e-money.

[72] Beside these four entities, there are actually two other entities covered under the proposal, namely the central banks (the European Central Bank and the national central banks) and member states when not acting as public authorities. However, these entities are less relevant to this chapter.

[73] Proposal for a directive on the subject matter: COM (2013) 48 final, 2013/0027 (COD) (7 February 2013).

[74] Under article 3(1) (b) and (c) of the proposed NIS directive.

[75] Under article 1(1) of the proposed NIS directive.

"market operators") providing services within the EU shall perform the following obligations. Firstly, to take appropriate measures, both technical and organizational, to mitigate the security risks of their systems. Such measures must be able to guarantee a security level appropriate to the risks exposed.[76] Secondly, to notify to the authority any security breaches having a significant impact to the systems.[77] When necessary, the competent authority may also require the service providers to make notification of any incidents or breaches of their system. For instance, when the incidents or breaches are in the public interest. Other provisions to strengthen the NIS include setting up the national competent authority, cooperation among the national competent authorities and the Computer Emergency Response Team (CERT), and to encourage the use of standards and other common technical specifications.

However, challenges arise when one tries to apply provisions under the proposed NIS directive to the Bitcoin system. Like the PSD and the proposal of PSD2, the main challenges come from the nature of the Bitcoin system that is a decentralized system without any central counterparty. To whom will the regulator impose the security requirements under article 14 of the proposed NIS directive? Who is the service provider (again, the proposed NIS directive uses the term "market operator") of the Bitcoin systems? First, one needs to define the definition and scope of service providers under the NIS directive. Such a definition, as laid down under article 3(8), consists of two players: providers of any information services and operators of critical infrastructures such as those in the area of energy, banking, transport or stock exchange. The former includes e-commerce platforms, payment gateways, social networks and application stores, while the latter includes electricity suppliers, railways and air carriers. However, it is difficult to apply such a definition and scope to the Bitcoin system. As Bitcoin is a peer-to-peer and decentralized system, no single player in the Bitcoin ecosystem serves as the provider of the system; neither exchanges, miners nor users do. Furthermore, the Bitcoin system is also not (yet) a critical infrastructure to the economy. Hence, who will

[76] Article 14(1) of the proposed NIS directive.

[77] Article 14(2) of the proposed NIS directive.

be responsible to implement the obligation imposed by article 14 of the proposed NIS directive?

On the narrower scope, one might be able to hold some players in the Bitcoin ecosystem liable for implementing the security obligation under article 14 of the proposed NIS directive. For instance, exchange providers in the Bitcoin system. As exchange providers basically provide service to users by providing platforms enabling users to exchange real money to Bitcoin and vice versa, they arguably satisfy the definition of the service providers under article 3(8) of the proposed NIS directive, in particular the providers of e-commerce platforms.[78] By putting the exchanges under the definition and the scope of service providers, it would be possible to impose the security obligations under article 14, which are to take appropriate measures to mitigate the security risks of their system and to notify to the authority of any security breaches. As security breaches at the exchanges occur over and over again, recently involving 12 exchanges including Mt. Gox that was considered the biggest exchange yet, bringing the exchanges under the proposed NIS regulatory framework will strengthen the security of the supporting systems of Bitcoin and create a better arrangement in dealing with breaches. In the end, if security breaches are able to be prevented, and if they have occurredare better managed, consumer protection in the Bitcoin system will be better preserved.

Conclusion

New innovative payments such as m-payments and the Bitcoin system expose different security issues: m-payments with new security risks and Bitcoin with the vulnerabilities of its supporting systems. In m-payments, the new security risks consist of the accumulation of the security risks embedded to mobile devices and the security risks of the payment platforms used, while the vulnerabilities of the Bitcoin supporting systems are in particular found in the systems of users and exchanges. Such security issues have given rise to the regulatory challenges in the EU, both the existing and proposed regulatory frameworks relating to payment systems.

[78] See Annex II of the proposed NIS directive. E-commerce platforms are explicitly mentioned as one of service provider designated under the proposed regulation.

M-payment security issues challenge the existing regulatory framework for not providing a framework that guarantees high security on the one hand, and encourages the usability of the systems on the other hand. This is reflected by two elements: adequate security requirements and sufficient consumer protection. The adequate security requirements are difficult to apply to m-payments for two reasons. Firstly, m-payment providers are varied—from banks to MNOs to app-based start-up companies—and most of them have, by nature, less or no expertise in dealing with the security and the security issues of payment systems. Secondly, the so-called third-party payment service providers are not yet covered by regulation. Using services provided by entities that are not yet covered by regulations exposes high risks to consumers. As for sufficient consumer protection, redress arrangements enabling consumers to seek remedies and limited liability for consumers under the existing framework do not entirely fit to the consumers of m-payments. For instance, the limited liability is too lost-or-stolen-instrument minded, whereas a mobile device as such is not a payment instrument. It is generally irrelevant for consumers to notify m-payment providers of any lost or stolen device. In addition, the maximum amount of liability for consumers up to EUR150 is too high considering the average value per transaction of m-payments amounted to EUR28.27 in 2014.

As for Bitcoin, particular security issues that might give rise to regulatory challenge consist of three parts: firstly, the Bitcoin system is not yet covered by regulation; secondly, although claimed to be the most secure, lost/stolen Bitcoin and breaches at exchanges keep occurring; and finally, there were some discussions on the technical flaws of the Bitcoin system. The existing regulatory frameworks in the EU say nothing about the Bitcoin system. Some governments issued a warning about risks embedded in using Bitcoin that consumers must be aware of. However, such a warning has no implication to address the Bitcoin thefts as it is not a legal instrument or legislative product. It is more an *ex ante* instrument for prevention rather than *ex post* instrument for remedy.

The proposed regulatory frameworks on payment systems seem promising for m-payments as there is a legislation imposing the general principles accompanied by a recommendation on the technical standards by SecuRe Pay Forum. However, the omission of the explicit wordings on the obligation to maintain strong security measures in the proposed

framework, replacing them instead by a reference to the proposed NIS directive, create uncertainty. In addition, the recommendation on the technical standards needs to be less rigid to let the m-payment flourish. With regard to the limited liability for consumers, the proposed reduction on the maximum amount of the liability from up to EUR150 to EUR50 is a good progress and therefore needs to be supported. However, the remaining issues, such as concerns of being too lost-or-stolen-instrument minded and the difficulties for consumers to seek redress from unauthorized transactions, remain unchanged and need to be addressed.

As for Bitcoin, the proposed framework on payment systems remains silent. However, the proposed NIS directive might be applicable to the Bitcoin system. Under this proposed directive, service providers shall take appropriate measures to mitigate the security risks of their systems and notify to the authority any security breaches having a significant impact to the systems. However, as Bitcoin is a peer-to-peer and decentralized system, it is impossible to determine the service provider of the system. As a result, the proposed NIS directive would not be enforceable to Bitcoin. One possible solution is to hold some players in the Bitcoin ecosystem liable for the implementation of the security obligation under the proposed NIS directive. For instance, exchange providers as they meet the definition and scope of service providers. In this manner, the security of the supporting systems of Bitcoin will be strengthened, and a better arrangement in dealing with security breaches will be created.

References

Bolt, W. (2012). *Retail payment systems: Competition, innovation, and implications*. De Nederlandsche Bank Working Paper No. 362 / December 2012.

Borchgrevink, J. (2014). Warning: GHash.IO is nearing 51 % – Leave the pool. *Crypto Coins News*. Reterived January 9, 2014 from https://www.cryptocoinsnews.com/warning-ghash-io-nearing-51-leave-pool/

Camenisch, J. L., Piveteau, J.-M., & Stadler, M. A. (1994). Security in electronic payment systems. Institute for Theoretical Computer Science, ETH Zurich. Available at http://www.ubilab.org/publications/print_versions/pdf/piv94b.pdf.

Chatain, P.-L. (2008). Integrity in mobile phone financial services, measures for mitigating Risks from money laundering and terrorist financing. *The World Bank Working Paper* No. 146. Washington DC.

Clarkson, E. C., Patel, S. N., Pierce, J. S., & Abowd, G. D. (2006). *Exploring continuous pressure input for mobile phones*. Georgia Institute of Technology, available at https://smartech.gatech.edu/bitstream/handle/1853/13138/06-20.pdf, last accessed on 28 April 2016

Desai, S. (2014). Mobile payment services: Security risks, trends and countermeasures. *RSA Conference 2014*, Asia Pacific & Japan.

Desjardins, J. (2014). How secure are bitcoins? *Visual Capitalist*. Reterived August 13, 2014, from www.visualcapitalist.com/secure-bitcoins/

European Central Bank. (2014). *Mandate of the European Forum on the Security of Retail Payments*. October 2014. Available at https://www.ecb.europa.eu/pub/pdf/other/mandateeuropeanforumsecurityretailpayments201410.en.pdf.

European Central Bank. (2013). *Recommendations for the security of mobile payments, draft document for public consultations*. Reterived 2013, from https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf?7f9004f1cbbec932447c1db2c84fc4e9

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

European Payments Council Newsletter. (2014). *EPC comments on the draft recommendation for the security of mobile payments developed by the European Forum on Security of Retail Payments.* April 29, 2014. Available at https://www.ecb.europa.eu/pub/pdf/other/mandateeuropeanforumsecurityretailpayments201410.en.pdf.

European Payments Council. (2014). *Overview mobile payments initiatives*. EPC091-14. Version 2.0. 2014.

European Commission, Directorate-General for Research and Innovation. (2013). *Final report from the expert group on retail sector innovation*. Reterived October 30, 2013, from http://ec.europa.eu/research/innovation-union/pdf/Report_from_EG_on_Retail_Sector_Innovation_A4_FINAL_2.pdf

European Payment Council. (2015). *Summer reading*: *Results of latest EPC poll reveal that instant payments are most likely trigger the next wave of innovation* (blog). August 07, 2015.

Herzberg, A. (2003). Payments and banking with mobile personal devices. *Communications of the ACM, 46*(5), 53–58 Chicago.

Information Systems Audit and Control Association (ISACA). (2011)._ Mobile payments: Risk, security and assurance issues. *An ISACA Emerging Technology*

White Paper. Reterived November 2011, from http://www.isaca.org/groups/professional-english/pci-compliance/groupdocuments/mobilepaymentswp.pdf

International Finance Corporation (IFC). (2011). *Mobile money study: Summary report*. Available at http://www.ifc.org/wps/wcm/connect/fad057004a052e-b88b23ffdd29332b51/MobileMoneyReport-Summary.pdf?MOD=AJPERES.

Kasiyanto S. (2016). Bitcoin's Potential for Going Manistream. Journal of Payments Strategy & Systems, Vol. 10(1), 28-39. March 2016.

Kasiyanto, S. (2015). Regulating peer-to-peer network currency: Lessons from Napster and payment systems. *Journal of Law, Technology and Public Policy, 1*(2), 40–73.

Kim, C., Tao, W., Shin, N., & Kim, K.-S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications, 9*(1), 84–95.

Linck, K., Pousttchi, K., & Wiedemann, D. G. (2006). *Security issues in mobile payment from the customer viewpoint*. MPRA Paper No. 2923. Available at http://mpra.ub.uni-muenchen.de/2923/.

Mallat, N. (2007). Exploring consumer adoption of mobile payments – A qualitative study. *Journal of Strategic Information Systems, 16*, 413–432.

Moody's. (2013). *Moody's analytics: The impact of electronic payments on economic growth*. Available at https://usa.visa.com/dam/VCOM/download/corporate/media/moodys-economy-white-paper-feb-2013.pdf.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Consulted 1.2012.

Ondrus, J., & Pigneur, Y. (2009). Near field communication: An assessment for future payment systems. *Information Systems and E-Business Management, 7*(3), 347–361.

Payment System Directive. *What it means for consumers*. Available at http://ec.europa.eu/internal_market/payments/docs/framework/psd_consumers/psd_en.pdf

Payment System Directive. (2007) *Commission encourages swift and coherent implementation at national level, press release IP/07/1914*. Reterived December 12, 2007, from http://europa.eu/rapid/press-release_IP-07-1914_en.htm?locale=en

Pegueros, V. (2012). Security of mobile banking and payments. *SANS Institute InfoSec Reading Room*. Available at https://www.sans.org/reading-room/whitepapers/ecommerce/security-mobile-banking-payments-34062.

Pousttchi, K., & Wiedemann, D. G. (2007). What influences consumers' intention to use mobile payments. *Mobile Communications Working Group*,

University of Augsburg. Reterived from http://www.marshall.usc.edu/assets/025/7534.pdf

Rode, L. (2006). Database security breach notification statutes: Does placing the responsibility on the true victim increase data security. *Houston Law Review, 43*, 1597.

Rosenfeld, M. (2012). *Analysis of hash-rate-based double-spending*. Latest version: December 13, 2012. Available at https://bitcoil.co.il/Doublespend.pdf

Schmiedel, H., Kostova, G. L., & Ruttenberg, W. (2012). The social and private costs of retail payment instruments: A European perspective. *ECB Occasional Paper* 137.

Schoenmakers, B. (1997). Basic security of the e-cash payment system. *Computer security and industrial cryptography*: *State of the art and evolution*, *LNCS series*. In B. Preneel and V. Rijmen (eds.) State of the Art in Applied Cryptography, Course on Computer Security and Industrial Cryptography, Leuven, Belgium, June 3–6, 1997, vol. 1528 of Lecture Notes in Computer Science, pp. 338–352. Springer-Verlag.

Sirer, E. G. (2014). *What did not happen at Mt. Gox*. March 01, 2014. Available onlineathttp://hackingdistributed.com/2014/03/01/what-did-not-happen-at-mtgox/.

Souppaya, M., & Scarfone, K. (2013). Guidelines for managing the security of mobile devices in the enterprise. *NIST Special Publication*, 800.

Sullivan, R. J. (2014). Controlling security risk and fraud in payment systems. *Federal Reserve Bank of Kansas City, Economic Review, 99*(3), 47–78.

TALOS Vulnerability Report. (2015). *MiniUPNP internet gateway device protocol XML parser buffer overflow*. Reterived September 15, 2015, from TALOS-2015-0035. http://talosintel.com/reports/TALOS-2015-0035/

Turban, E., & Brahm, J. (2000). Smart card-based electronic card payment systems in the transportation industry. *Journal of Organizational Computing and Electronic Commerce, 10*(4), 281–293.

Visa Europe Risk Management. (2014). *Secure mobile payment systems, recommendations for building, managing and deploying*. Visa Europe.

Winklevoss, C. *What may have happened at Mt.Gox*. Reterived from https://winklevosscapital.com/what-may-have-happened-at-mt-gox/

Wile, R. (2014). *One of Bitcoin's strongest backers reveals the two big reasons why it's still not mainstream*. Reterived July 20, 2014, from http://www.businessinsider.com/fred-wilson-on-bitcoin-2014-7?IR=T

8

EU Data Protection and Future Payment Services

Gloria González Fuster

Abstract With the second Payment Services Directive, the European Union embraces new payment services by tackling some of the legal challenges they trigger. Personal data protection is one of the most critical of such challenges, and it is itself in a crucial transition period. A General Data Protection Regulation is indeed to replace the current Data Protection Directive, coinciding with a progressive consolidation of the EU right to personal data protection. This contribution explores the current and upcoming regulatory challenges in this field. After introducing the EU legal framework on personal data protection, it reviews the data protection provisions of the updated Payment Services Directive, and discusses them critically. The findings are then explored considering the wider context of mobile payments, as well as "alternative currencies".

G. González Fuster (✉)
Law, Science, Technology and Society (LSTS), Vrije Universiteit Brussel (VUB), Belgium

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_8

Introduction

European personal data protection is in a crucial period of transition. The key legal instrument establishing personal data protection rules applicable across the European Union (EU), dating back from 1995—Directive 95/46/EC, generally known as the Data Protection Directive-,[1] is to be replaced by a General Data Protection Regulation consolidating a high level of protection in light of post-Lisbon EU fundamental rights standards. The upcoming General Data Protection Regulation faces the challenge of providing effective protection and legal certainty in a society where the processing of personal data is quantitatively and qualitatively more important than ever, and where new technologies and practices continuously raise new, and sometimes complex, legal questions.

Payments are at the forefront of some of these developments. Unsurprisingly, therefore, personal data protection surfaced as a critical subject of debate in the legislative process leading to the adoption of the second Payment Services Directive. The second Payment Services Directive aims to tackle regulatory and security challenges posed by emergent mobile payment services, and to guarantee a competitive payments card market taking into account the increasing use of online and mobile payments.

This contribution explores the regulatory challenges of ensuring personal data protection in the face of evolving payment services. It first introduces the main features of the EU legal framework for personal data protection. Second, it describes how personal data protection concerns impacted the drafting of the second Payment Services Directive, reviews the resulting provisions on the matter, and investigates which issues failed to be addressed. These findings are then put in the larger context of the evolution of payment services, giving particular attention to mobile payments and the issue of "alternative currencies" such as the Bitcoin system. Finally, the chapter highlights the significance of the upcoming EU legislative steps in this field.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L281, 23 November 1995, 31–50.

The Moving EU Data Protection Landscape

When it was adopted in 1995, the Data Protection Directive aimed to guarantee the harmonization of national laws to allow for the free movement of personal data among all Member States, contributing to the functioning of the European single market, while mandating the respect of the fundamental rights and freedoms of individuals, and in particular of their right to privacy. Yet, the level of harmonization of national laws and practices achieved by the Directive has been limited.

In 2012, the European Commission put forward a proposal for a General Data Protection Regulation to replace Directive 95/46/EC,[2] aiming at strengthening the level of harmonization in the area. The proposed General Data Protection Regulation was designed in an institutional setting very different from the one of 1995: whereas the Data Protection Directive was a Community instrument primarily pursuing the creation of the single market, and incidentally concerned with the respect of rights and freedoms of individuals, the proposed Regulation is firmly grounded in the fundamental rights obligations of the EU, as redefined by the entry into force of the Lisbon Treaty in 2009.

The Lisbon Treaty, indeed, transformed the EU approach to personal data protection by, first, granting legally binding force to the EU Charter of Fundamental Rights, which explicitly enshrines a EU fundamental rights to the protection of personal data (in its Article 8),[3] and, second, incorporating into the EU Treaties a mandate for the European Parliament and the Council to lay down the rules relating to this right and to the free movement of such data (Article 16 of the Treaty on the Functioning of European Union). The Regulation proposed by the European Commission in 2012 aims to give substance to the EU legislator's obligation to legislate on this fundamental right.

---

[2] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (*General Data Protection Regulation*), COM(2012) 11 final, 25 January 2012, Brussels.

[3] On this right, see: Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Dordrecht: Springer, 2014).

The EU Charter recognizes that the EU fundamental right to the protection of personal data is granted to "everyone",[4] and that it entails that personal data "must be processed fairly" (that is, in compliance with applicable rules determining the exact obligations of those responsible for the processing), always "for specified purposes" (in accordance with what is known as the "purpose limitation principle") and "on the basis of the consent of the person concerned or some other legitimate basis laid down by law" (that is, based on a legitimate ground, which could be the consent or another ground).[5] Additionally, the Charter states that the individuals to whom the data processed relates have a "right of access" to such data, as well as "the right to have it rectified" when appropriate.[6] Finally, it stipulates that compliance with these rules "shall be subject to control by an independent authority".[7] All in all, Article 8 of the EU Charter foresees thus a right based on the imposition of a series of obligations on those who process personal data (the "data controllers" and "processors"), the granting of subjective rights to the individuals to whom the data relates (the "data subjects"), and the existence of independent authorities charged with controlling compliance (the "data protection authorities").

Discussions on the proposed General Data Protection Regulation have coincided in time with the progressively increasing reliance on the EU fundamental right to the protection of personal data by the Court of Justice of the European Union. In this sense, in 2014 and 2015 the Court of Justice delivered a series of important judgments taking as starting point the EU Charter of Fundamental Rights, and documenting the significance of this new right.

Three rulings illustrate well the current prominence of the fundamental rights dimension of EU personal data protection law. In April 2014, in the *Digital Rights Ireland* judgment, the Luxembourg Court annulled

[4] Article 8(1) of the EU Charter of Fundamental Rights.

[5] Article 8(2) of the EU Charter of Fundamental Rights.

[6] Ibid.

[7] Article 8(1) of the EU Charter of Fundamental Rights.

Directive 2006/24/EC,[8] which imposed a general retention of data generated or processed in connection with the provision of publicly available electronic communications services and public communications networks services.[9] In the *Google Spain and Google* ruling of May 2014,[10] the Court, confronted with a reference for preliminary ruling on the so-called "right to be forgotten", asserted that search engine operators are obliged to accept removing certain types of data from the list of results displayed following a search made on the basis of a person's name linking to web pages, published by third parties and containing information relating to that person—and this also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful. In October 2015, in the *Schrems* judgment,[11] the Court declared that the "Safe Harbour" Decision of the European Commission,[12] adopted in 2000 to facilitate the transfer of personal data from the EU to the USA by private companies, was invalid—generating by the same token much legal uncertainty as to which transfers of personal data to the USA might actually be valid.

Whereas the upcoming General Data Protection Regulation is to constitute the future cornerstone of EU personal data protection law, the legislative procedure directed towards its adoption has coincided with the discussion by EU institutions of other, sector-specific provisions on personal data protection. This has been the case, precisely, of the data protection clauses accompanying the review of the Payment Services Directive.

---

[8] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105, p. 54.

[9] Judgment of the Court (Grand Chamber) of 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*.

[10] Judgment of the Court (Grand Chamber) of 13 May 2014, C-131/12, *Google Spain and Google*.

[11] Judgment of the Court (Grand Chamber) of 6 October 2015, Case C-362/14, *Schrems*.

[12] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the Safe Harbour privacy principles and related Frequently Asked Questions issued by the US Department of Commerce.

Data Protection for the New Payment Services Directive

The revision of the Payment Services Directive[13] was formally launched with a legislative proposal made public by the European Commission in 2013[14] thus, in the middle of discussions on its proposal for a General Data Protection Regulation. The review of the Payment Services Directive had the general objective of promoting competition, efficiency and innovation in the e-payments field, and taking into account the increasingly important role played by non-bank service providers. The proposed rules aimed to make online payments safer, notably by laying down data protection rules for all payment service providers.

The European Data Protection Supervisor (EDPS), an independent supervisory authority responsible for advising EU institutions on privacy-related policies and legislation, had already been informally consulted by the European Commission during the preparation of the legislative proposal. After its official publication, the European Commission formally submitted the text to the EDPS for consultation, leading to the publication of an Opinion[15] where the EDPS underlined the need for a series of changes, in light of both the current EU data protection framework and the foreseeable developments in the area.

The EDPS insights were particularly supported during the legislative procedure by the European Parliament. After negotiations with the Council and having reached an inter-institutional agreement in May

[13] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L319, 5 December 2007, 1–36.

[14] European Commission, *Proposal for a Directive of the European Parliament and of the Council on payment services in the market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC*, COM(2013) 547 final, 24 July 2013, Brussels.

[15] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on a Proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market Amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and Repealing Directive 2007/64/EC, and for a Regulation of the European Parliament and of the Council on Interchange Fees for Card-Based Payment Transactions*, 5 December 2013, Brussels.

2015, in October 2015 the European Parliament backed up the adoption of a revised text including important amendments related to personal data protection.[16]

Data Protection in the New Payment Services Directive

The original draft of the European Commission foresaw a whole chapter devoted to "Data Protection" (namely, Chap. 4), which actually consisted of a single Article entitled "Data Protection" (Article 84), which merely stated that "[a]ny processing of personal data for the purposes of this Directive shall be carried out in accordance with Directive 95/46/EC", the national rules transposing Directive 95/46/EC, and Regulation (EC) No 45/2001, which mirrors the Data Protection Directive's provisions but is addressed at EU institutions and bodies.[17] As such, the proposed Article 84 simply confirmed the general applicability of the mentioned instruments.

Negotiations between the European Parliament and the Council eventually transformed the "Data Protection" Article proposed by the European Commission into a new Article (now Article 94), composed of two paragraphs. The first one, i.e. Article 94(1) of the updated Payment Services Directive, establishes 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", before adding that such processing as well as any

[16] European Parliament, *Legislative Resolution of 8 October 2015 on the proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC* (*COM(2013)0547 – C7-0230/2013–2013/0264(COD)*) (Ordinary legislative procedure: first reading), P8_TA(2015)0346.

[17] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L8, 12 January 2001.

other processing of personal data must comply with Directive 94/46/EC and Regulation (EC) No 45/2001—an idea that is actually also recalled in the preamble.[18]

The main novelty of this finally agreed version of Article 94 is that it generally establishes the safeguarding of the prevention, investigation and detection of payment fraud as a legitimate basis for the processing of personal data, to be imperatively respected as such by Member States. The origin of this stipulation can be traced back to a Recital of the draft that had been published by the European Commission, which, however, stated more narrowly that payment service providers should be allowed to process personal data relating to persons involved in payment fraud. Thus, the original Recital did not support any processing of personal data for the prevention, investigation and detection of payment fraud, but only the processing of personal data related to persons actually participating to or connected with such fraud. Lifting this requirement potentially opens the door to the processing, in the name of payment fraud prevention, investigation or detection, of personal data of persons completely unrelated to payment fraud, for instance through data mining or profiling techniques that would generally aim at automatically distinguishing fraudulent from non-fraudulent payments.

In any case, this special mandate directed to Member States to imperatively allow for the processing of personal data for the safeguarding of the prevention, investigation and detection of payment fraud as a legitimate basis for the processing of personal data has to be regarded as complementing the freedom granted to Member States by Directive 95/46/EC to adopt, when necessary, legislative measures to restrict the scope of some data protection obligations and rights in the name of the prevention, investigation, detection and prosecution of criminal offences.[19]

The second paragraph of the updated Payment Services Directive, Article 94(2), establishes that "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". This provision, if read in isolation, could be interpreted as gen-

[18] Recital 89 of the second Payments Service Directive.

[19] Art. 13(1)(d) of Directive 95/46/EC.

erally conditioning any processing of personal data by payment service providers to the obtaining of the explicit consent of the user, who presumably is also the person to whom the data relate—that is, the "data subject" in EU data protection law terms.

Article 94(2) triggers a set of questions related to its consistency with the wider EU personal data protection legal framework, as well as with the very Article 94(1) that precedes it. In this sense, as previously noted, the consent of the data subject is, as a matter of fact, only one of the possible bases that can constitute a legitimate ground for the processing of personal data in EU law. As described above, Article 8 of the EU Charter of Fundamental Rights enshrines at the highest level the principle that personal data can be processed "on the basis of the consent of the person concerned", but also on the basis of "some other legitimate basis laid down by law". In accordance with the Data Protection Directive, which is indisputably applicable, as confirmed by Article 94(1), data controllers may also process personal data, *inter alia*, when the processing is necessary for the performance of a contract (or in order to take steps prior to entering into a contract),[20] or when processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.[21] These bases could appear to be, in many cases, fully relevant to justify the completion of a payment transaction.

The question is, thus, whether Article 94(2) of the new Payment Services Directive can exclude the applicability of any of these Data Protection Directive provisions as legitimate basis in the context of payment services, or whether it merely recalls that, in absence of any other legitimate basis, payment service providers shall only process data on the basis of the explicit consent of the user (who, supposedly, is also the "data subject" at stake—other legal issues might be triggered if at any point personal data related to different individuals is processed).

In any case, the cumulative reading of Article 94(2) of the new Payment Services Directive and of the Data Protection Directive's provisions

[20] Art. 7(b) of Directive 95/46/EC.

[21] Except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject requiring protection (Art. 7(f) of Directive 95/46/EC).

on consent obliges us to interpret that, whenever the payment service providers base their processing on the consent of the user, such consent shall be explicit—as required by Article 94(2) of the revised Payment Services Directive—but also freely given, specific, informed and unambiguous, as required by Articles 2(h) and 7(a) of Directive 95/46/EC.[22]

This leads to the problem of how to comply in practice with these requirements, for instance in the context of emerging modes of payment, such as mobile payments. It is indeed unclear how the data subjects can be fully and specifically informed about the complex data processing practices taking place in such situations, and how could their consent be freely given (or refused) to the payment service provider when they have, for instance, committed to pay for a certain service or product. From this perspective, entrusting to the data subject's consent the effective (personal data) protection of the users of emergent payment services might turn out to be, eventually, an unfortunate policy strategy.

Missing Data Protection Safeguards

The general framework of personal data protection in EU law, currently epitomized by Article 8 of the EU Charter together with the Data Protection Directive (soon to become the General Data Protection Regulation), defines the general provisions bounding all data controllers operating in the payments field, including those whose activities might not fall under the scope of the revised proposed Payment Services Directive. The general EU data protection regime should thus ultimately allow tackling any privacy and data protection challenges not directly addressed by sector-specific rules.

The EDPS had emphasized in 2013 that it was not enough for the proposed Payment Services Directive to allude to the general applicability of EU personal data protection provisions, but that it was necessary, instead, for the new instrument to supplement such general provisions by detailing additional concrete and substantial safeguards.[23]

[22] For a discussion on consent and its role in EU personal data protection law, see: Eleni Kosta, *Consent in European Data Protection Law* (The Hague: Martinus Nijhoff, 2013).

[23] Opinion of the EDPS (2013): 3.

The need for not only reasserting, but rather reinforcing personal data protection safeguards in relation to payment services, and especially emerging payment services, can be justified by the fact that privacy and personal data protection are generally highlighted as genuine concerns of the population in this area, not only in the EU,[24] but globally. In the USA, for instance, Google Inc. and Google Payment Corporation are facing a class action related to the sharing of personal information collected through the Google Wallet system.

Reinforced safeguards might also be required by the numerous specific challenges linked to the factors such as multiplication of operators involved, which renders particularly complex the attribution of responsibility to the different actors, their relations with data subjects, and the monitoring of compliance with applicable rules.

The 2012 European Commission's Green Paper *Towards an integrated European market for card, internet and mobile payments* described the security of retail payments as a crucial prerequisite for payment users and merchants alike, highlighting data protection as a key issue in the field.[25]

In practice, the simultaneous (but not fully coincidental in time) review of the Payment Services Directive and the Data Protection Directive appears to have had a negative impact on facilitating the inclusion of sector-specific additional safeguards for payment services. It was understandably difficult for the EU legislator to agree on creating any specific rules for the sector while not having reached a general agreement on the future General Data Protection Regulation.

The EDPS's call for concrete substantial provisions has thus in reality basically translated into a Recital on the agreed revised Payment Services Directive, which is rather detailed but, still, only declaratory. Recital 89, indeed, after a reminder that Directive 95/46/EC is generally applicable whenever personal data is processed, points out that, "[i]n particular", whenever personal data is processed for the purposes of the updated Payment Services Directive, "the precise purpose should be specified,

[24] In this sense, see, for instance: BEUC, The European Consumer Organisation, *Towards an Integrated European Market for Card, Internet and Mobile Payments*: *European Commission Consultation on the Green Paper* (2012): 2.

[25] European Commission, *Green Paper Towards an Integrated European Market for Card, Internet and Mobile Payments*, COM 941 final, 1 November 2012, Brussels, (2011): 19.

the relevant legal basis referred to, the relevant security requirements laid down in Directive 95/46/EC complied with, and the principles of necessity, proportionality, purpose limitation and proportionate data retention period respected".

The usefulness of this Recital, which is not actually backed up by specific provisions in the Directive, might be limited. It must be stressed, in any case, its insistence of the concept of purpose limitation, as the Recital first recalls that whenever personal data is processed the "precise purpose" of the processing must be specified, and afterwards alludes to the need to respect the purpose limitation principle. This principle, however, is in fact one of the data protection principles more regularly put under pressure by industries such as the banking industry, generally keen to process data for not originally specified purposes such as marketing.[26]

Additionally, Recital 89 also purports that "data protection by design and data protection by default should be embedded in all data processing systems" developed and used within the framework of the Payment Services Directive. This assertion, which is also not echoed by any provision of the Directive itself, evokes as a matter of fact two notions, the meaning of which is yet to be defined in EU law: "data protection by design" and "data protection by default". These two notions are expected to be present in the final General Data Protection Regulation, but it is only when the agreed text is settled that it will possible to evaluate their legal significance and the possible impact of this reference in the Directive's preamble.

Minimizing Data Exchanges: A Real Privacy Measure

As a matter of fact, a particularly positive development for the protection of the data protection rights of individuals took place during the legislative procedure not under the "Data Protection" chapter of the revised Payment Services Directive, but in the context of its provisions on confirmation on the availability of funds by payment services. Here,

[26] Mario Viola De Azevedo Cunha, *Market Integration Through Data Protection*: *An Analysis of the Insurance and Financial Industries in the EU* (Dordrecht: Springer, 2013), p. 25.

the text supported by the European Parliament foresees a limitation of the information to be provided by an account servicing payment service when, upon the request of a payment service provider issuing card-based payment instruments, it has to confirm whether an amount necessary for the execution of a card-based payment transaction is available on the payment account of the payer.

Article 65(3) of the agreed text, indeed, establishes that such confirmation shall consist "only in a simple 'yes' or 'no' answer and not in a statement of the account balance", as opposed to "a statement of the account balance". Furthermore, the content of the answer (that is, the "yes" or "no"), shall not be stored, neither used for purposes other than for the execution of the card-based payment transaction. The provision states that this must be so "[i]n accordance with Directive 95/46/EC", which can be seen as a reference to the Data Protection Directive's principle according to which personal data processing shall never be "excessive" in relation to the purposes for which they are processed.[27]

By integrating this data-minimization principle into the very design of the functioning of payment services, the new Payment Services Directive can be seen as de facto incorporating, at least to some extent, the notions of data protection *by default* and *by design* understood as an imperative to analyse and address data protection concerns before they surface. Supporting this view, the European Commission had actually already relied in its 2012 Green Paper on the idea of having to conceive of authentication mechanisms for payment transactions "designed from the outset to include the necessary measures to ensure compliance with data protection requirements".[28]

Mobile Payments in the Waiting Line

What is more debatable, however, is whether the new Payment Services Directive effectively offers any substantive, by default or by design, response to the specific data protection challenges raised by the increas-

[27] Art. 6(c) of Directive 95/46/EC.

[28] European Commission, Ibid., 19.

ing use of payment systems allowing to pay through remote or near technologies, for instance using a mobile phone. Mobile payments can have a direct impact on the quantity and quality of data processed during the provision of payment services, bringing into the discussion different types of operators with different types of business practices[29]; as a matter of fact, they typically take the shape of complex ecosystems with very varied market participants.[30]

From a EU law perspective, such mobile payments fall not only under the scope of sector-based payment services rules: they actually also operate somewhere at the crossroads of two additional data protection regimes, that is, the general regime as described by the Data Protection Directive (to be replaced, as noted, by the General Data Protection Regulation), and the one delineated by the so-called e-Privacy Directive, Directive 2002/58/EC[31] establishing sector-based, specific rules for the telecommunications sector. The latter notably puts forward special rules for some categories of data such as "traffic" and "location" data, in the understanding that insuring the fundamental rights and freedoms of individuals requires a particularly strict processing of this type of data.

The data protection framework for the telecommunications sector is expected to be reviewed by the EU legislator as soon as an agreement is reached on the General Data Protection Regulation, in view of bringing them in line. Such review will most probably have to consider the issue, pending already for a number of years, of whether some providers of internet services shall be submitted to compliance of rules that were originally only directed at providers of telecommunications operators.

---

[29] Chris Jay Hoofnagle, Jennifer M. Urban, and Su Li, "Mobile Payments: Consumer Benefits & New Privacy Concerns", *BCLT Research Paper* (2012): 2.

[30] Richard Kemp, "Mobile Payments: Current and Emerging Regulatory and Contracting Issues", in *Computer Law & Security Review* 29 (2013): 176.

[31] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31 July 2002, p. 37–47, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L337, 18 December 2009, p. 11–36.

Some of these internet service providers are, in reality, also active in (or now entering) the field of payment services, in what has been described as a profound shift in the relationship between customers and payment service providers.[32] That upcoming, post-General Data Protection Regulation legislative debate might be, perhaps, the moment when a discussion of an effective and detailed regulation of data protection in mobile payments is feasible.

Mobile Payments and EU Data Protection

To map out the regulation of data protection issues related to mobile payments in the EU it is thus necessary to take into account the general EU personal data protection rules (including primary and secondary rules), sector-based rules for payment services and sector-based rules for privacy and data protection in the telecommunications sector, as well as the synergies between them. In practice, the relationships between these different types of rules can actually take different shapes depending on the Member State, and on the different approaches that might surface at national level. Despite the existence of EU personal data protection rules and the foreseen adoption of a General Data Protection Regulation that will dramatically boost harmonization, indeed, the degree of harmonization in this area is not yet complete, and will still not be complete while Member States might transpose differently the e-Privacy and the Payment Services Directives, allowing (still) for national divergences.[33]

An interesting example of national legal framing of data protection issues related to mobile payments can be found in Italy. The Italian data protection authority (Garante per la Protezione dei Dati Personali) published in 2014 a Resolution on remote mobile payments services,[34] detail-

[32] Hoofnagle, Urban and Li, Ibid., 9.

[33] On fear of persistent lack of full harmonization of EU data protection obligations, see: European Banking Federation (EBF), *EBF Position on the European Commission's Green Paper 'Towards an Integrated European Market for Card, Internet and Mobile Payments*, 10 April 2012.

[34] Provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di mobile remote payment, 22 maggio 2014, Pubblicato sulla Gazzetta Ufficiale n. 137 del 16 giugno 2014.

ing substantive guidance on the basis, most notably, of the provisions of the Data Protection Directive (that is, the general data protection regime), the e-Privacy Directive (sector-specific rules for the telecommunications sector) and the review of the Payment Services Directive (sector-specific rules for the payments services sector), which was ongoing at that time. Taking stock of the variety of players typically involved in mobile payment services, as well as of the variety and quantity of data generated by these services, it describes obligations in terms of information, data storage and data security. In relation to consent, the Resolution sets out that the consent of the user is not required for the processing of personal data related to the transaction itself, but it shall be necessary for any marketing-related processing of data surrounding the use of the mobile payment service.

At EU level, useful guidance emanating from the data protection authorities can be found in the Article 29 Working Party 2013 Opinion on apps on smart devices.[35] The Opinion notably identifies the different types of data that can potentially be accessed by applications installed in smart devices,[36] and recommends maximum granularity for the information to be provided to users.[37] In relation to consent, it points out that the processing of information about payments that "is strictly necessary in order to perform [a] contract with this specific user"[38] does not require the user's consent, even if other data processing activities will.

Effective data protection safeguards appear to be, in any case, one of the prime concerns of prospective adopters of mobile payment services. This idea has been already integrated by some banks, which see their expertise in the area as a competitive advantage in the field.[39] In the USA, a country lacking a comprehensive regulation of privacy and data protection equivalent to EU standards, some services have actually nevertheless encoun-

[35] Article 29 Working Party (2013), *Opinion 02/2013 on apps on smart devices*, WP 202, 27 February 2013, Brussels.

[36] Ibid., p. 8.

[37] Ibid., p. 27.

[38] Ibid., p. 16.

[39] See, for instance: Thomas F. Dapp, Antje Stobbe, and Patricia Wruuck, *The Future of* (*mobile*) *Payments*: *New* (*online*) *Players Competing with Banks*, Deutsche Bank Research, 20 December 2012: 26.

tered privacy-related resistance from some users.[40] The frictions between emerging mobile payment and EU privacy and personal data protection might appear as somehow inevitable when one considers that for some actors the collection of data other than strict transaction data, as well as its further processing (with the aim of increasing advertising revenue), is not a side activity but an essential dimension of their business model.[41]

EU Data Protection and Alternative Currencies

Looking into emergent payment services, an issue prompting peculiar challenges for the regulation of privacy and personal data protection is the use of "alternative currencies" such as the Bitcoin. Privacy and personal data protection issues related to alternative currencies relying on decentralised systems are different from those relevant in traditional banking models,[42] which does not mean, however, that they do not exist. In traditional models, it is openly accepted by those involved in transactions that personal data about them will be processed by at least a third party, who is thus clearly responsible for compliance with personal data protection rules.

In a system like the Bitcoin system, however, transactions are, in principle, supposed to be "anonymous", that is, un-linkable to anybody. Information about such "anonymous" transactions must nevertheless be publicly released, because it is such openness that constitutes the very foundation of the system's trust. This triggers the question of the limits of such "anonymity": once the information is publicly available, it might be possible for a third party to trace back one or more transactions to a concrete individual, for instance using other information also publicly available, or crossing such data with data in their hands—for instance,

[40] Concretely, the Google Wallet application has prompted a lawsuit related to Google's payment service sharing of personal information with app developers.

[41] Charles Gibney et al., "International Review: Mobile Payments and Consumer Protection", Financial Consumer Agency of Canada, January (2015): iv.

[42] See, in this sense: Satoshi Nakamoto, *Bitcoin*: *A Peer-to-Peer Electronic Cash System* (2008), available online: http://nakamotoinstitute.org/bitcoin/#selection-7.4-13.16.

information including Internet Protocol (IP) addresses.[43] The limitations of the anonymity guaranteed by the system are actually commonly acknowledged, and even if there are different ways in which users of the Bitcoin system can increase the chances of their transactions remaining "anonymous", the system does not aim to guarantee anonymity.

As soon as data regarding a transaction are potentially linkable to a concrete individual, rules on the protection of personal data must be regarded as applicable. In accordance with the general EU data protection regime, indeed, personal data protection rules apply to "personal data" understood not only as information related to an identified individual, but also to an "identifiable" natural person, meaning anyone "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[44]

From this perspective, it is clear that anybody (a third party) who would process data about Bitcoin transactions and have the possibility to link such data to concrete individuals shall be regarded as a "data controller" for the purposes of EU data protection law, and thus be responsible for compliance with such rules insofar as it processes personal data.

A different set of questions regards determining whether the data in the system itself could also be regarded as "personal data" to the extent that, under certain circumstances, they might, at least after being made publicly available, relate to identifiable sets of individuals. If that were the case—and this certainly cannot be absolutely excluded a priori—it would lead to the issue of determining who is the responsible "data controller" for the data processed and made publicly available through the peer-to-peer system. Possible approaches would be to consider each and every user equally responsible,[45] but also to take into account the possible responsibility of internet service providers (ISP) involved.[46] This debate is still very much open.

---

[43] For a description of the various possible ways to identify Bitcoin users, see: Fergal Reid and Martin Harrigan "An Analysis of Anonymity in the Bitcoin System" in Yaniv Altshuler et al. (Eds.) *Security and Privacy in Social Networks*, (Dordrecht: Springer, 2013), pp. 197–223.

[44] Art. 2(a) of Directive 95/46/EC.

[45] Suggesting this option: Artus Krohn-Grimberghe and Christoph Sorge, "Practical Aspects of the Bitcoin System", *The Computing Research Repository* (*CoRR*), August 2013.

[46] On this issue, see: Mario Viola de Azevedo Cunha, Luisa Marin, and Giovanni Sartori, "Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web", *International Data Privacy Law* 2, No. 2 (2012): 50–67.

Concluding Remarks

This contribution has shown that the updated Payment Services Directive tackles data protection issues linked to emergent payment services in a somehow uneven manner. Whereas some positive advances have been identified, the truth is that many important questions remain open, and some questions have actually been raised by the very agreement on some problematic formulations of the Directive's provisions.

Although the situation might be explained by the persistent uncertainties due to the long and persistent negotiations on the General Data Protection Regulation, the deficiencies described appear to be particularly untimely as the Court of Justice of the European Union continues to assert the importance of the EU fundamental right to the protection of personal data. The Court of Justice's strong position should act as a persuasive factor inviting the EU legislator to provide for a complete and effective protection of the rights of individuals also in the payment services sector. If the final text of the General Data Protection Regulation does not completely achieve this objective, the eyes will certainly turn to the subsequent review of the e-Privacy Directive.

All in all, it is clear that the increasingly stronger general rules for data protection in the EU will eventually require equally stronger sector-based rules, bringing the necessary clarity and legal certainty to the field, and preventing the surfacing of problematically disparate national rules.

References

Article 29 Working Party. (2013). *Opinion 02/2013 on apps on smart devices*. WP 202, 27 February. Brussels.

BEUC, The European Consumer Organisation. (2012). *Towards an integrated European market for card, internet and mobile payments*: *European Commission Consultation on the Green Paper.*

European Banking Federation (EBF). (2012). *EBF position on the European Commission's Green Paper 'towards an integrated European market for card, internet and mobile payments*. 10 April 2012.

European Commission. (2012a) *Green Paper towards an integrated European market for card, internet and mobile payment*s. COM(2011) 941 final, Brussels: 1.11.2012.

European Commission. (2012b). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (*General Data Protection Regulation*), COM(2012) 11 final, Brussels: 25.1.2012.

European Commission. (2013). *Proposal for a Directive of the European Parliament and of the Council on payment services in the market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC.* COM(2013) 547 final. Brussels: 24.7.2013.

European Data Protection Supervisor (EDPS). (2013). *Opinion of the European Data Protection Supervisor on a proposal for a Directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and repealing Directive 2007/64/EC, and for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions*. Brussels: 5.12.2013.

European Parliament. (2015). *Legislative Resolution of 8 October 2015 on the proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC* (*COM*(*2013*)*0547 – C7-0230/2013–2013/0264*(*COD*)) (Ordinary legislative procedure: first reading), P8_TA(2015)0346.

Dapp, T. F., Stobbe, A., & Wruuck, P. (2012). *The future of* (*mobile*) *payments*: *New* (*online*) *players competing with banks.* Deutsche Bank Research, 20 December 2012.

De Azevedo Cunha, M. V. (2013). *Market integration through data protection: An analysis of the insurance and financial industries in the EU*. Dordrecht: Springer.

De Azevedo Cunha, M. V., Marin, L., & Sartori, G. (2012). Peer-to-peer privacy violations and ISP liability: Data protection in the user-generated web. *International Data Privacy Law, 2*(2), 50–67.

Gibney, C., et al. (2015). *International review*: *Mobile payments and consumer protection*. Financial Consumer Agency of Canada, January 2015.

González Fuster, G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Dordrecht: Springer.

Hoofnagle, C. J., Urban, J. M., & Li, S. (2012). Mobile payments: Consumer benefits & new privacy concerns. *BCLT Research Paper*.

Kemp, R. (2013). Mobile payments: Current and emerging regulatory and contracting issues. *Computer Law & Security Review, 29*, 175–179.

Kosta, E. (2013). *Consent in European data protection law*. The Hague: Martinus Nijhoff.

Krohn-Grimberghe, A., & Sorge, C. (2013). Practical aspects of the Bitcoin system. *The Computing Research Repository* (*CoRR*), August 2013.

Nakamoto, S. (2008). *Bitcoin*: *A peer-to-peer electronic cash system.* Available online: http://nakamotoinstitute.org/bitcoin/#selection-7.4-13.16

Reid, F., & Harrigan, M. (2013). An Analysis of anonymity in the Bitcoin system. In Y. Altshuler, et al. (Eds.), Security and privacy in social networks (pp. 197–223). Dordrecht: Springer

9

The Classification of Virtual Currencies and Mobile Payments in Terms of the Old and New European Anti-Money Laundering Frameworks

Carolin Kaiser

Abstract Both virtual currencies and mobile payments are rapidly growing, novel developments in the global payments industry. These developments create challenges for regulators when it comes to fitting the new technology into the old legal framework. In some cases, the legal framework has to be amended to cover new technological developments. In this chapter, the European anti-money laundering framework in its older shape (Directive 2005/60/EC) and in its newest incarnation (Directive (EU) 2015/849) is examined. The shortcomings of the directives are to be exposed and possible ways around these shortcomings are explained.

Introduction

Virtual currencies are rapidly growing. While the first successful virtual currency, Bitcoin, was only introduced in 2008, there are now several hundred virtual currencies in existence, and a whole new market emerging. Virtual currencies, as most emerging technologies, come with

C. Kaiser (✉)
PhD researcher, Rijksuniversiteit Groningen, the Netherlands

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_9

great potential as well as difficult challenges. The challenge that will be addressed in this paper is the classification of virtual currencies in terms of European anti-money laundering legislation.

As virtual currencies are an entirely new phenomenon, unforeseen by legislators, the law does not yet reflect even their existence. A decentralized payment system without formal institutions is simply not envisioned. However, bringing virtual currencies under the umbrella of anti-money laundering legislation is crucial if the abuse of the technology as a tool for money laundering is to be prevented. Now that the European legislator has passed a fourth directive on anti-money laundering, it would have been an ideal point in time to remedy the omission of virtual currencies in the currently applicable framework and thus bring the European anti-money laundering framework truly up-to-date.

A similarly new, though not quite as revolutionary, payment instrument is mobile payments, or m-payments. Mobile payments are payments made using a mobile device, such as a smart phone or tablet.

Proponents and early adopters of new technologies often face problems when applying the existing legal framework to the new technology. The law is often lagging a few steps behind the state of the art. This is also, to a certain extent, the case for mobile payments and virtual currencies. The uncertainty of the legal situation is creating problems for businesses and private parties who wish to use either of these technologies.

The purpose of this paper is to shed light on the legal provisions regarding anti-money laundering law as applicable to virtual currencies and mobile payments. To this end, this paper begins by comparing the Third (Directive 2005/60/EC) and the new Fourth Anti-Money Laundering Directive (Directive (EU) 2015/849) regarding their coverage of virtual currencies and mobile payments and analysing the position of businesses wishing to engage with these instruments in the anti-money laundering framework. For this purpose, this chapter will, after a preliminary short discussion of both virtual currencies and mobile payments in general and of why regulation of these instruments is needed, examine the treatment of each instrument in the Third Anti-Money Laundering Directive and in the new Fourth Anti-Money Laundering Directive, and finally present its conclusions on the inclusion of virtual currencies and mobile payments in the framework.

The Need for Regulation

Virtual Currencies

Both virtual currencies and mobile payments are new payment instruments, to which the general public is slowly getting accustomed.

Virtual currencies are an emerging phenomenon. While the idea of virtual currencies is not new, the idea could for a long time not be properly transposed into a software solution, which would be secure enough to use for financial transactions. In 2008, a person or group of persons under the pseudonym Satoshi Nakamoto introduced a concept for a technology he called Bitcoin,[1] a decentralized virtual currency based on a peer-to-peer system, a public ledger, and cryptography. This concept was peer-reviewed and launched in 2009, and is now the first widely adopted and securely working multipurpose virtual currency. Since the launch of Bitcoin as the prototype of virtual currencies, hundreds of similar systems have been developed,[2] though Bitcoin remains the largest and most successful network.

In Bitcoin and other virtual currencies that are based on the same protocol, other users in a peer-to-peer system clear transactions, and all transactions are recorded in a publicly accessible ledger, which, together with the use of cryptography to secure transactions, allows the Bitcoin system to provide an environment for secure financial transactions without the need for a bank.[3] The system is essentially made up of users running the protocol, some being more involved as "miners", who keep the ledger up-to-date and are rewarded for their services with newly minted units. With no formal connection between the users, as these users are spread all over the world only connected through the internet, and as there is no legal entity to represent the Bitcoin system on the whole, oversight of one government over the system itself can hardly be realized.

---

[1] Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, https://bitcoin.org/bitcoin.pdf.

[2] Such as Litecoin, Peercoin, Freicoin and Dogecoin, to name but a few, collectively called "altcoin" as they are alternatives to the predominant Bitcoin.

[3] Grinberg, Reuben, "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science & Technology Law Journal* 4, (2001): 159–208, 160 f.

Virtual currencies are thus marked by their lack of a connection to any state, and by the privacy they can afford to their users. Virtual currencies, unlike fiat currencies, are not issued by any state or government, and also not regulated and overseen by a central bank, but rather issued and maintained by a group of people running the ledger and system with their computer power. The privacy afforded by virtual currencies is connected to this lack of government involvement, in that virtual currencies generally lack an institution that could be compared to a bank and which would carry out supervision and monitoring tasks, such as the tasks required by anti-money laundering legislation.

The general public is only slowly becoming aware of virtual currencies, and it is still a mystery to many how and why they work and hold value. However, criminals have been among the early adopters of the new technology. Several websites have been launched, which provide a market place for sellers and buyers of illegal material, such as drugs and guns.[4] Bitcoin, as the most widely adopted virtual currency, is used in some of them as a means of exchange, as the strict monitoring of bank accounts and credit card transactions compared to the current lack of government oversight over virtual currencies made it the best available tool to complete criminal financial transactions online.[5] At the same time, a large number of legitimate businesses, among which a large number of online businesses but also brick-and-mortar offline shops, wish to accept virtual currencies as payment in exchange for their goods and services, but do not know which obligations they need to comply with.

Furthermore, Europol reports that Bitcoin is being adopted rapidly for criminal transactions of all descriptions. In 2015, according to Europol's information, Bitcoin was used in more than 40 % of all transactions between criminals, followed by other payment systems such as PayPal.[6] Also when demanding payments from cybercrime victims, Bitcoin is the

[4] Luther, William J., "Regulating Bitcoin: On What Grounds?", (2015): 19 Available at SSRN: http://ssrn.com/abstract=2631307.

[5] Financial Action Task Force (FATF), "Guidance for a risk-based approach – Virtual Currencies", (2015): 33 http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

[6] Europol, "The Internet Organized Crime Threat Assessment (IOCTA)" (2015): 46.

preferred avenue, used in about a third of all extortion cases.[7] Interestingly, in the context of money laundering, it is reported that Bitcoin is used only in few cases.[8]

In view of this potential for misuse of virtual currencies for the purposes of illegal transactions as well as the potential benefit of virtual currencies to legitimate businesses, it is important to bring virtual currencies in line with European anti-money laundering legislation, in order to reduce the risks as much as possible.

To summarize, there are thus three main reasons to regulate virtual currencies. These are, in the first place, to bring virtual currencies in line with economic or monetary policy objectives despite their lack of any apparent connection with any state government, in the second place, to protect consumers from the risks of engaging with a technology they may not understand, and finally, to prevent misuse of the technology for illegal transactions such as money laundering.[9] This chapter is concentrating on the latter reason.

Mobile Payments

As we have seen, virtual currencies are thus a completely new financial transaction system, with a completely novel underlying code. Mobile payments are also a new payment method, but while virtual currencies break with most traditions, mobile payments give the traditional banking services a new aspect with a modern technological base and integration.

A mobile payment is, to put it into simple words, a payment made using a mobile device.[10] The mobile device to be used for the payments in this case contains software to carry out the transactions. This software is commonly called a mobile wallet. Wallets are computer files which contain all information needed to digitally carry out a financial transac-

[7] Europol, Ibid, 47.

[8] Ibid.

[9] For a thorough discussion, see also Luther, Regulating Bitcoin, 3.

[10] European Payments Council (EPC), "Overview Mobile Payments Initiatives", 2014. EPC091-14, Version 2.0, p. 10, s.v. Mobile payment service.

tion, including information on available payment services and accounts as well as personal information of the user, and optionally a number of other documents and information relating to payments, such as addresses, electronic signatures and integrated applications such as loyalty schemes, etc.[11]

There are a large number of wallet providers, that is, businesses which offer software solutions for wallets, usually in the form of applications. The wallet file can either be stored directly on the user's mobile device or be stored on the provider's servers and accessed remotely.[12]

Two main types of mobile payment systems have been identified. The first type is "mobile payment services", enabling "non-bank and non-securities account holders to make payments with mobile phones".[13] The second is "mobile money services", in which "subscribers are able to store actual value on their mobile phones".[14] These two systems are the most interesting in terms of anti-money laundering. In the former option, the wallet file offers a mobile connection to the user's financial accounts, whereas the latter stores credits directly in the wallet file. The distinction between these two systems is important, as they are treated differently by the law, but the term "mobile payments" is often used as a general term covering both of these versions.

There are different ways in which a mobile payment can be transacted. In the first place, there are mobile remote payments, which are carried out on a mobile device via a network, such as wireless or mobile internet connection, independently of the location of the parties to the transaction.[15] Also playing a more and more decisive role in mobile payments are so-called mobile proximity payments, in which a proximity technology is used, such as near field communication (NFC) or QR (quick response)

[11] EPC, Ibid., 16.

[12] Ibid.

[13] Financial Action Task Force (FATF), "Money Laundering Using New Payment Methods", (2010): 18 http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf.

[14] Ibid.

[15] EPC, Overview Mobile Payments Initiatives, 11.

codes, which require both parties to the transaction to be in the same location.[16]

The use of mobile payments is increasing rapidly. *Jana Valant* compiled a number of statistics, which show that circa 60 % of Europeans owned a smartphone in 2015, though the numbers vary considerably among the Member States.[17] The European Commission reports that there were 67 mobile broadband subscriptions for every 100 EU residents in 2014.[18] This would be the reason why the mobile commerce sector is growing so quickly, at a spectacular 42 % per annum,[19] currently representing 14 % of the total e-commerce sector.[20]

The widespread use of smartphones and tablet PCs and the increasingly secure applications that are being developed for the use of mobile payments make this technology an attractive tool for financial transactions. Mobile payments allow the user to carry out payment transactions without the need to carry cash or credit/debit cards.[21] Many users find it very convenient to be able to have their smartphone integrate as many features as possible, thereby making it unnecessary to carry other devices. Also, the integration of the payments feature into existing smartphones may result in more flexibility and lower costs for users.[22] Furthermore, mobile payments are facilitating access to the unbanked and underbanked population in many developing countries in Africa and Asia, where a formal banking infrastructure is practically inaccessible to large parts of the population, but the mobile network is growing with unprecedented speed.

There are, however, also disadvantages to mobile payments, the most important and pressing of which are security concerns. The massive growth of the sector and the correspondingly increasing demand were met by a large number of different software solutions for mobile pay-

[16] Ibid.

[17] Ecommerce News, quoted in Valant, Jana, "Consumer Protection Aspects of Mobile Payments", European Parliamentary Research Service, European Parliament Briefing (2015): 2.

[18] The European Commission, quoted in Valant, Ibid., 2.

[19] Ecommerce News, quoted in Ibid.

[20] The European Commission, quoted in Ibid.

[21] Valant. Ibid., 4.

[22] Ibid.

ments. The wallets that are being offered and made available are often, however, in the early stages of development, and thus not necessarily entirely secure. There are also privacy concerns, as a large amount of data can be shared during the transaction, including not only information on the transaction itself, but also geographical location data and information on the service or item that is to be sold or bought, and it is not always clear to the user, who has access to this information.[23]

Mobile payments have not yet been connected to a specifically high risk of money laundering, despite the rapid growth of these systems and their predominant use in countries with poor financial regulation and oversight. How high or low the risk of money laundering in mobile payments is, depends essentially on in how far the mobile payment service provider follows anti-money laundering legislation, as outlined below.

It is important to note that the definition of mobile payments so far evolves around fiat currency, and excludes virtual currencies from its scope. The details of the omission of virtual currencies are discussed below. Virtual currencies, however, are also frequently used on mobile devices, either remotely, or proximately, using QR codes. Virtual currencies can be included in some mobile wallets, integrating the two technologies.

The Third Anti-Money Laundering Directive 2005/60/EC

The purpose of anti-money laundering legislation is summarized in Recital 1 of the Fourth Anti-Money Laundering Directive (EU) 2015/849, which states that "[f]lows of illicit money can damage the integrity, stability and reputation of the financial sector, and threaten the internal market of the Union as well as international development." This recital goes on to stress that this issue should best be addressed at Union level.

In other words, the purpose of this legislation is to take the proceeds of an already committed crime from the perpetrator, thereby making

[23] Valant, Ibid., 5

the commission of the crime less attractive.[24] The predicate offences to money laundering can be of vastly different natures, ranging from the sale of illegal material to illegal gambling, prostitution, corruption and tax crimes. Which predicate offences can trigger anti-money laundering mechanisms can be very different in each Member State.[25] The European legislator explains his involvement in Recital 3 of Directive 2005/60/EC, which is repeated in Recital 2 of the Fourth Anti-Money Laundering Directive, with the following formula: "In order to facilitate their criminal activities, money launderers and terrorist financers could try to take advantage of the freedom of capital movements and the freedom to supply financial services which the integrated financial area entails, if certain coordinating measures are not adopted at Union level."

The formerly applicable (until May 2015) European approach to anti-money laundering is codified in the Third Anti-Money Laundering Directive 2005/60/EC. This directive is the implementation on a Union level of the international anti-money laundering standards, which are to a great extent developed under the leadership of the Financial Action Task Force (FATF) in their 40 Recommendations for the prevention of money laundering and the IX Special Recommendations for the combating of the financing of terrorism.[26]

That the Third Anti-Money Laundering Directive does not mention virtual currencies at any point is not surprising. The directive was passed in 2005, while Bitcoin, the first widely successful virtual currency, was only launched in 2009. However, virtual currencies may still be covered by the directive to a certain extent.

---

[24] Cuéllar, Mariano-Florentino, "The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance", *Journal of Criminal Law and Criminology* 93, (2003): 311–465, 2003; Stanford Public Law Working Paper No. 64, 323 ff.

[25] See the list of "serious crimes in directive 2005/60/EC, article 3(5)(a-f), and in directive (EU) 2015/849, article 3(4)(a-f).

[26] Financial Action Task Force (FATF), "International standards on combating money laundering and the financing of terrorism & proliferation ("The FATF Recommendations")", http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf, (2012): 118

The Material Scope

The directive, beginning with a general appeal to Member States to prohibit the tasks of money laundering and the financing of terrorism, includes a very broad definition of money laundering.

According to Article 1 (2) of the directive, money laundering can take the shape of a number of different intentional actions:

> (a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action; (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity; (c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity; (d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

Article 1 (3) extends this definition to acts "even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country."

Terrorist financing is defined in Article 1 (4), which states that "'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism."

The definitions of money laundering as well as terrorist financing are thus very broad, covering a range of activities and actions as well as different means. It is important to note that the definition of money laundering does not, in fact, speak of "money" at all, but rather utilizes the

term "property". The definition of terrorist financing, in much the same way, uses the term "funds". The directive includes a definition of the term "property" in Article 3 (3). According to that definition, "'property' means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets." Although the directive includes no definition of the term "funds", the FATF recommendations including a definition of the term which is almost identical to that of "property" in the directive.[27] Thus the terms cover in essence the same subject matter.

The use of the term "property" rather than "money", and the inclusion of intangible assets in the definition of the term "property" leaves no doubt that virtual currencies are in principle covered by the directive. Virtual currencies should be subsumed under the term "assets of every kind", especially as incorporeal and intangible assets are explicitly included in the definition (Article 3 (3)).

The Personal Scope

The actors that are addressed by the directive are manifold. Essentially, the directive addresses all actors either transferring value as a part of the nature of their business, or handling large amounts of cash or valuable items in commerce, employing several catch-all phrases throughout Article 2.

In detail, the principal addressees are credit institutions (Article 2 (1)) and financial institutions (Article 2 (2)), which cover various entities, such as banks, currency exchange offices, money transmitters and remittance offices.[28] Furthermore, a number of legal or natural persons, who in their line of business handle large sums of money or deal in valuable property, are obligated to comply with the measures set forth in this directive. The natural and legal persons addressed are, among others,

[27] Ibid.

[28] Article 2 (2) refers to points 2–12 and 14 of Annex I of Directive 2000/12/EC. See also FATF (2015) p. 6.

auditors, accountants and tax advisors, but also notaries, real estate agents and casinos (Article 2 (1) (a-f)).

Furthermore, all natural and legal persons acting as sellers of goods must observe the customer due diligence (CDD) measures outlined in the directive, when they accept cash payments of EUR15,000. The threshold applies both when the amount is transferred in a single transaction and when the sum of a series of transactions that appear to be linked amount to EUR15,000 or more.[29] Cash transactions are included not only because the origins of cash are very difficult to trace, but also because luxury goods are easily moved and re-sold at little loss, thus also used as a vehicle for funds transfer.

As virtual currencies thus clearly fall into the definition of "property", the natural and legal persons to whom the directive applies must observe their obligations under the Third Anti-Money Laundering Directive when dealing with virtual currencies in just the same way as when they deal with other property. There two branches of business that have particularly evolved around virtual currencies.

In the first place, there are online exchange offices. Online exchanges are the main entry and exit point for users of the virtual currency economy.[30] While there are several ways to acquire virtual currencies, the majority of users will visit an online exchange service, where Euro or other fiat currency can be exchanged for virtual currency. Therefore, online exchange offices are acting in much the same way as foreign currency exchange offices, with the small difference that they operate by necessity mainly online, as virtual currencies have no physical manifestation. In order to be covered by the directive, the exchanges need to fall under the definition of financial institution in Article 3 (2) (a-f). Article 3 (2) (a) includes "an undertaking other than a credit institution which carries out one or more of the operations included in points 2 to 12 and 14 of Annex I to Directive 2000/12/EC, including the activities of currency exchange offices (bureaux de change) and of money transmission

[29] Article 2 (1) (e).

[30] European Banking Authority (EBA), "EBA Opinion on virtual currencies", 2014 https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf, p. 40.

or remittance offices". As was just explained, online currency exchange offices dealing with virtual currencies should be treated in the same way as analogue currency exchange offices, and these are mentioned explicitly in this paragraph. Online exchange offices thus fall under Article 2 (1) (2) of the directive and must be licensed or registered in the Member State in which they are established, in accordance with Article 36 (1). The online exchanges established within the territorial scope of the directive must observe European anti-money laundering legislation and comply with the obligations stipulated therein.[31]

Another major branch of businesses that utilizes virtual currencies are online gambling services. The various platforms make up a large part of the transactions in virtual currencies. The directive applies to "casinos" (Article 2 (1) (f)), but the term "casino" only covers brick-and-mortar casinos, leaving "other areas of gambling vulnerable to miss-use by criminals."[32] Online gambling services thus to a large extent fall out of the scope of the Third Anti-Money Laundering Directive.

While these two groups of actors are at this point in time most prevalent among the businesses plugging into the economies of the different virtual currencies, the possibility cannot be excluded that other businesses will follow as the use of virtual currencies expands.

Mobile payment service providers will be classified as financial institutions as money transmission services, as these services are used to transfer value between accounts. In the case of mobile money services, such as M-Pesa, the service provider issues a certain sort of prepaid credit, which is transacted via the mobile device. In this case, the provider also acts as an issuer of means of payments within the meaning of point 5 of Annex I of Directive 2000/12/EC (in force at the time), and thus falls under the definition of financial institution in Article 3 (2) (a) of Directive 2005/60/EC.

[31] Cf. FATF, The FATF Recommendations, 12 ff.; Europol, The Internet Organized Crime, 47.

[32] European Commission, "Proposal for a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing" COM (2013) 45 final (2013): 10.

Customer Due Diligence and Reporting

Customer due diligence measures are carried out at various stages of a business relationship, as listed in Article 7. Customer due diligence measures are applied in the first place before the start of a new business relationship, or when there is reason to doubt "the veracity or adequacy of previously obtained customer identification data".[33] Furthermore, they are applied when a customer wishes to transact a sum of EUR15,000 or more, both when this sum is transferred in a single transaction or in a series of transactions that seem to be linked, as outlined above. Lastly, a customer will undergo due diligence checks whenever "there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold".[34]

Customer due diligence measures comprise, in the first place, the identification of a customer and the verification of the customer's identity, using documents from official sources. When there is a beneficial owner, this person must be identified, and his identity verified as well. Furthermore, when a business relationship is to be established, the institution or person involved must identify the "purpose and intended nature of the business relationship".[35] Once the relationship is established, all ongoing transactions are to be continually monitored to make sure that the information gathered on the customer and the expected business relationship continue to be accurate.[36]

The levels of diligence with which these obligations must be carried out range from simplified to enhanced due diligence, depending on the subject matter of the transactions and the parties involved.[37]

However, this practical application of the anti-money laundering measures as prescribed in Chaps. 2 and 3 of the directive is hampered by several factors. Virtual currencies are designed to be decentralized, lacking a

[33] Article 7 (d).

[34] Article 7 (c).

[35] Article 8 (1) (c).

[36] Article 8 (1) (d).

[37] Mitsilegas, Valsamis and Gilmore, Bill, "The EU legislative framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards", *International & Comparative Law Quarterly* 56, no. 1 (2007): 119–140, 127.

central authority that would clear transactions and collect information. This ledger is maintained by the collected effort of a large number of loosely connected users who support the system, but who cannot be classified as a "financial institution" in the terms of the directive. There is no entity involved that could be compared to the banks, which are obliged by anti-money laundering legislation to carry out the bulk of the identification and monitoring tasks for transactions. Instead, information is collected in a public ledger, which records all transactions carried out over the system. This decentralization and lack of a central entity strengthens the privacy that the systems afford.[38] The ledger records all transactions, but the parties to the transactions are only identified by the public keys used to encrypt the transaction. Information on who is behind the public keys is not readily available.

Finally, a grave problem for the enforcement of anti-money laundering measures against users of a virtual currency system is the fact that virtual currencies are by necessity a phenomenon existing exclusively online, on the internet. The businesses plugging into the economy can deliver their services to customers worldwide, while being established anywhere in the world, with the risk that service providers suitable for money laundering operations will establish themselves in jurisdictions with little or no oversight. This problem, however, is a problem of internet governance in general, and addressing this issue here would go beyond the scope of this article. The European anti-money laundering legislation only covers entities established within the territory of a Member State.

Customer due diligence obligations are thus carried out by the main actors connecting to the environment of the virtual currency in question, such as exchange services, online gambling services, and other businesses dealing in virtual currencies.

Providers of mobile payment services face the same obligations to identify customers and monitor their accounts to counter money laundering activity. How well providers are able to identify their customers depends on the type of service offered. Mobile payment services that are connected to the client's bank account carefully verify the client's iden-

[38] See for proposed solutions for more compliance FATF, Guidance for a risk-based approach – Virtual Currencies, 14.

tity before access can be facilitated. Mobile money services working with prepaid credits can face different challenges. If the credits can only be obtained from the service provider, the service provider can also take appropriate measures to establish the identity of the buyer. If the credits can be bought in other places, as in the case of M-Pesa, where credits can be bought in retail shops in the form of scratch-cards, there are often gaps in the identification of customers. This latter system is not, however, prevalent in Europe.

There has, so far, been no case law in which the European Court of Justice had an opportunity to advance its views on how to classify either virtual currencies or mobile payments in terms of the European anti-money laundering framework.

The Fourth Anti-Money Laundering Directive (EU) 2015/849

The Third Anti-Money Laundering Directive was to a large extent based on the FATF recommendations of 2003. On 5 February 2013, the Commission proposed a Fourth Anti-Money Laundering Directive, to bring the framework in line with the newest version of the FATF Recommendations, which were updated in 2012.[39] This proposal was duly adopted and the new Fourth Anti-Money Laundering Directive came into force in May 2015.

The Broadened Scope

The personal scope of the directive has not changed dramatically compared to the previous directive. The Fourth Anti-Money Laundering Directive clarifies and expands the personal scope in a few instances, for example by replacing the term "casinos" with "gambling services", to close any loopholes that a narrow definition of the term "casinos" may

[39] FATF, The FATF Recommendations.

have left open.[40] Online gambling is thus brought within the scope of the directive.

Furthermore, tax crimes have been added to the list of predicate crimes to money laundering. Funds derived from "tax crimes related to direct taxes and indirect taxes" are punishable with a term of imprisonment of at least six months, if the Member State has a system of minimum thresholds, or punishable with a term of imprisonment of more than one year, if maximum terms are stipulated in the code (Article 3 (4) (f)). The inclusion of tax crimes is closing a lacuna left in Directive 2005/60/EC. That the crimes must be serious enough to be "punishable by deprivation of liberty or a detention order" of a certain amount is a measure to ensure that only crimes of a certain gravity are included in the list of predicate offences to money laundering, and should be strictly observed in order to prevent minor offences to be included and the meaning of the term "serious crimes" to be watered down. Inclusion of minor offences would not only disproportionately affect financial secrecy in general and the liberty and privacy of transferees, but also create "an additional administrative burden" and increase the costly oversight measures implemented by the financial industry.[41]

The threshold for cash payments has been lowered from previously EUR15,000 to EUR7,500. It had been reported that the former high threshold was facilitating the use of luxury goods for money laundering.[42] Legal and natural persons accepting cash payments for goods will thus fall into the scope of the directive more often.

In addition, the new text is rounded off with a stricter treatment of politically exposed persons (PEPs) (Article 3 (9)), in order to address the risk of laundering the proceeds of corruption. The previous directive only covered high government officials from foreign countries, while the Fourth Anti-Money Laundering Directive extends the definition of PEPs to include also domestic PEPs as well as high officials in interna-

[40] COM (2013) 45 final, 9 f.; FATF, Guidance for a risk-based approach – Virtual Currencies, 12 ff.

[41] Eurofinas, Eurofinas Observations on the Commission's Proposal for a Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (COM(2013) 45 final), (2013): 4, http://www.eurofinas.org/uploads/documents/positions/AML/Eurofinasobservations-final.pdf.

[42] COM (2013) 45 final, 9.

tional organizations. The list of offices that are covered include also members of the supreme courts and other high courts whose decisions are not normally subject to appeal, members of the boards of central banks, ambassadors, high-ranking military officials and persons charged with the management or supervision of publicly owned enterprises (Article 3 (9) (a-h)). All transactions involving persons falling into the definition of PEP are subject to enhanced CDD measures (Article 20). However, the sum of PEPs is rather large, and constantly changing. Especially for small financial institutions, it is impossible to maintain an own list of persons, thus obliging them to rely on lists prepared by commercial enterprises, which creates a considerable financial burden.[43] Additionally, even when a commercial list of PEPs is used by the financial institution, the accuracy of this list is generally not guaranteed, leaving the risk with the financial institution.[44] A reliable public list of PEPs, prepared preferably on a European level, has been called for already under the old framework, but has so far not been realized.

Furthermore, information on beneficial owners of companies and other legal persons is required. The beneficial owner is "any natural person(s) who ultimately owns or controls the customer" (Article 3 (6)). Where legal persons and constructions using legal entities are involved in financial transactions, "the natural person who exercises ownership" must be identified (recital 12 f.), in order to prevent natural persons from hiding their identity behind a construction of legal persons. While this is a noteworthy development which has been applauded widely, it is as yet not certain how financial institutions are to determine the beneficial owner of companies. Also, constructions involving legal persons can be very complex, and a chain of legal persons established in several different countries can separate the beneficial owner from the transaction at hand. The impact on financial institutions is as yet unclear.[45]

The previously missing reference to data protection provisions was added in Articles 42, 43, and 45 of the Fourth Anti-Money Laundering Directive. However, the reference is rather declaratory in nature. Explicit

[43] Eurofinas, Eurofinas Observations, 7.

[44] Ibid.

[45] Ibid.

measures ensuring that the data collected in CDD measures is protected, and prescriptions on how this protection is to be achieved are regrettably still missing. On the whole, a higher protection of the data of the vast majority of users of financial services who are not involved in money laundering operations or the financing of terrorism would have been desirable, but the present text again falls short in this respect.

Unfortunately, the text does not explicitly include online gambling services using virtual currencies, nor does it explicitly cover exchange offices dealing in virtual currencies. The text of the directive has been updated, and the explanatory memorandum to the directive particularly refers to "the potential for misuse of new technologies to conceal transactions and hide identity",[46] but it still never mentions virtual currencies specifically.

The New Risk-Based Approach

Besides the slightly broadened scope, the main innovation of the new directive is the new emphasis on the risk-based approach. The concept of risk-sensitive CDD is not entirely new. The Third Anti-Money Laundering Directive allows for a gradation in the extent of the CDD measures to be applied in each individual case, based on how the customer, business relationship, product or transaction in question is assessed (Article 15 f). However, the Third Anti-Money Laundering Directive still set rather rigid categories, which did not allow for much flexibility on the part of the Member States and financial institutions. In the Fourth Anti-Money Laundering Directive, however, this risk-based approach would be implemented on three levels.

In the first place, the Commission will assess the risks of money laundering and terrorist financing within the internal market, and assess the risk resulting from cross-border activities (Article 6 (1)). Based on its findings, the Commission is to publish a report on the identified risks, to assist Member States and obliged entities in countering the risk of money laundering (Article 6 (3)).

[46] COM (2013) 45 final, 4.

Secondly, Member States are obliged to carry out a national risk assessment (Article 7). They "will be required to identify, understand and mitigate the risks facing them" on a national basis,[47] if necessary with help on a supranational level. The information thus gathered will then be shared among the Member States. The Commission calls this the "starting point for the risk-based approach", which may trigger responses on a Union level to risks reported by individual Member States.[48]

Finally, besides the national risk assessment carried out by Member States and the assessment of the Commission, all natural and legal persons falling into the scope of the directive will be required to assess the money laundering risks associated with the activities they undertake (Article 8).[49] The results of the assessment must be documented and shared with the competent supervisory entities for review. The obliged entity would, however, retain full responsibility for their decisions based on the risk assessment.[50]

The Commission goes on to stress that the risk-based approach would increase efficiency, as the available resources would be employed on the areas, which the different rounds of risk assessment have identified as being especially vulnerable.[51] None of these reports have as yet been forthcoming.

What the application of the risk-based approach will mean for users and providers of virtual currency services and mobile payment services cannot be predicted. However, a preliminary analysis is presented below.

The Need for Further Integration of New Payment Methods into the Legal Framework

The question remains whether anything has changed for the users of virtual currencies and mobile payments with the adoption of the new directive.

---

[47] Ibid, 10.

[48] Ibid. See also FATF, Guidance for a risk-based approach, 8 ff.

[49] COM (2013) 45 final, 10. See also FATF, Guidance for a risk-based approach, 12 ff.

[50] Ibid.

[51] Ibid.

Virtual Currencies

Just as its predecessor, the text of the directive does not explicitly mention virtual currencies at all, not even in the recitals. The position of businesses dealing in virtual currencies as well as their users thus continues to be uncertain. The Commission did mention the "potential for misuse of new technologies to conceal transactions and hide identity"[52] when it first introduced the proposed text of the directive, but did not elaborate on which technologies it refers to and how these new technologies should be brought under the umbrella of the proposed directive to mitigate the risks.

The Third Anti-Money Laundering Directive, as was stated above, was passed four years before the launch of the first successful virtual currency. The emergence of the new system was thus unforeseeable for the regulators at the time. The directive reflects a reality in which few big players dominate the market for financial transactions. It places emphasis on large established banks, credit card companies, and other transaction services,[53] to clear transactions and carry out CDD checks on their customers.

However, the Fourth Anti-Money Laundering Directive has been passed at a point when virtual currencies are receiving a high level of attention, and gaining in value and expanding their user bases rapidly, also because of their prominently being used in money laundering.[54] Passing the new directive without so much as a reference to virtual currencies thus seems a rare omission, and a lost chance to create legal certainty.

Virtual currencies, however, are likely just beginning to conquer the market in online payments and will continue to grow considerably in the coming years. The low transaction costs allow for micropayments, and the liquidity and basis on the internet could make them an ideal tool for mass-market e-commerce.[55] The low cost and convenience of using virtual currencies has the potential to shake the established order

[52] Ibid., 4.

[53] Such as PayPal and Western Union.

[54] See also EBA, EBA Opinion, 38 ff.

[55] Grinberg, Bitcoin: An Innovative Alternative, 160 f.

of a market dominated by few large players to the very core. Many businesses have already seen this potential and acted accordingly. New start-ups connected to virtual currencies are established rapidly. At the same time, the legal environment surrounding virtual currencies is highly ambiguous, and rules concerning not only the anti-money laundering obligations, but also taxation and other obligations faced by businesses in their particular industries need to be updated and amended to reflect the new situation.[56] While the rules do apply to businesses working with virtual currencies and businesses established so far have learned to arrange themselves rather well with the obligations conferred on them, it would be a vast improvement if the European lawmaker could bring himself to spelling out the obligations falling to businesses dealing with virtual currencies and acknowledging the existence of those systems.[57] By creating legal certainty and implementing simple rules for anti-money laundering obligations to be undertaken by services plugging into the virtual currency environment, Europe could position itself as a pioneer for a centre for virtual currencies and other online payment systems.

Therefore, the lack of mention of virtual currencies in the text of the directive is regrettable, as clear statements would have created legal certainty for the users and businesses intending to engage with the virtual currency network and community. At the same time, however, this lack of explicit regulation might still be better than overregulation.

Risk assessments carried out on the national level as well as by obliged entities will likely draw a very mixed picture of digital currencies. Here, the novelty and short acquaintance of many Member States with virtual currencies, coupled with the notoriety of the few money laundering

[56] Cf. FATF, Guidance for a risk-based approach, 8 ff. Major problems are caused for example by the fact that countries classify virtual currencies differently, as units of account comparable to foreign currencies as in Germany, or as assets comparable to gold and other commodities used for investments. See FATF, Guidance for a risk-based approach, 15 for an outline of the approach of several different countries, and Gup, Benton E. (2014) 'What is money? From commodities to virtual currencies/Bitcoin' Available at SSRN: http://ssrn.com/abstract=2409172, for an interpretation based on US American law.

[57] Ibid, 4: '[T]he rapid development, increasing functionality, growing adoption and global nature of VCPPS [virtual currencies] make national action to identify and mitigate the ML/TF risks presented by VCPPS a priority." Note that the FATF and this paper come to the same conclusion for different reasons.

cases in which virtual currencies have been employed (notably the recent Silk Road case) may potentially distort the view onto virtual currencies in some Member States and cause them to classify virtual currencies in general as a high-risk vehicle.[58] Furthermore, it seems likely that the risk-based approach provided for in the Fourth Anti-Money Laundering Directive will lead to fragmentation of the law, with different legal situations in each Member State.

In general, regulators all over the world seem insufficiently educated on virtual currencies, and are in many cases strongly biased against virtual currencies. Luther quotes several American government officials with statements showing an extreme distrust of the Bitcoin system.[59] The situation in Europe is very similar in this regard, with many warnings and negative advice from high official authorities.[60] The danger that states may simply classify all operations involving virtual currencies under the risk-based approach of Directive (EU) 2015/849, is thus imminent.[61]

Much of the negative image of virtual currencies can be traced back to the large amount of media attention given to the online market place Silk Road, where users could buy and sell illegal material, such as drugs, counterfeit documents, etc. As cash transactions, which would have been no doubt preferable for their anonymity, are not an option in online transactions, the site was an early adopter of Bitcoin, which facilitates a higher protection against discovery than credit cards or regular bank transactions. Although it is demonstrated that only a small number of all transactions in the Bitcoin system are illegal transactions,[62] the reputation clings to all virtual currencies to this date.

---

[58] Foreshadowed by Ibid., 6, 8 ff.

[59] Luther, Regulating Bitcoin, 19. See also EBA, EBA Opinion, 43 ff.

[60] The European Central Bank's reports on virtual currencies may serve as examples, with a strong bias towards painting a dark picture of virtual currencies, see European Central Bank (2015), 'Virtual currency schemes – a further analysis', https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf; the FATF is just as focused on the risks of virtual currencies, see FATF, Guidance for a risk-based approach.

[61] FATF, Guidance for a risk-based approach, 31 f.

[62] Luther, Regulating Bitcoin, 20. Luther goes on to stress that the United States dollar is still by far the favoured currency for illegal transactions.

Mobile Payments

The situation of mobile payments as well as mobile money services in the European Union is a bit clearer. Lacking the innovative structure of a decentralized virtual currency, they fit more or less nicely into the existing framework.

Mobile payments are, under the existing framework as amended by the Fourth Anti-Money Laundering Directive, financial service providers as defined in Article 3 (2) of the directive. Therefore, the obligations set forth in the directive, in particular the CDD and reporting obligations, apply also to service providers of mobile payments or mobile money services in the same way as to all other obliged parties under the directive. In addition to the obligations set forth in the anti-money laundering directive, mobile payment service providers must also follow the terms and obligations set forth in the Payment Services Directive.

As the applicable directives are being amended one by one by the European lawmaker, it is likely that mobile payments will be explicitly addressed in the new directives, as has already been done in Regulation 2015/847. This is a great advantage for providers of mobile payment services, as they can profit from the legal certainty provided by a harmonized European framework.

However, as with any new technology, mobile payment service providers are facing challenges when the existing legal framework is applied to them. The challenges lie, in the case of mobile payment service providers, to a large extent in making the system secure and protect their users' financial data. The amount of data potentially accessible and shared when using mobile payments or mobile money services applications on their mobile device,[63] are a great data protection concern to users and regulators. Several potential data protection and consumer protection risks have been identified, from which the developers of currently available applications are still ill-equipped to protect their users.[64] Among those problems are not only data leaks due to security breaches on the part of

[63] Valant, Consumer Protection Aspects, 5.

[64] Valant, Ibid., 4 ff.

the operator, but also possible man-in-the-middle attacks and phishing.[65] Another problem which might hamper development of mobile payments applications in the future is the lack of interoperability between existing service providers and platforms.[66]

The new risk-based approach will also very likely have an effect on mobile payments. But where virtual currencies have been involved in high-profile cases of criminal transactions already and are often associated with criminal transactions by laypersons, providers of mobile payment services do not have to deal with such a history. The risk assessment will concentrate on the customer's personal risk profile as assessed by the provider based on the information collected and the business relationship entered into, and other factors such as the country in which the recipient is located. As the whole sector of mobile payments is only starting to grow in Europe, however, the risk assessment will depend largely on the experiences customers, providers, law enforcement, and regulators make with this new technology over the next few months and years.

In summary, the challenges faced by regulators, developers and users at this point are to a less extent of a regulatory nature, than rather a developmental lag. Although they are gaining rapidly in acceptance and are becoming more and more popular with the general public, the underlying technology on which these mobile services are based are still in their infancy. As the legal framework applicable to mobile payments and mobile money service providers is comparatively clear and easily applicable, the technical challenges are most likely going to be more prominent in the development of mobile payments and mobile money applications.

Conclusion

In conclusion, the situation of virtual currencies in the legal framework on Union level remains uncertain. The situation of mobile payments is legally certain, but developers, users and regulators are confronted with technical difficulties at present and in the future.

[65] Valant, Ibid., 5 f.

[66] Valant, Ibid., 6.

It is regrettable that the European legislator has allowed the chance and opportunity to create more legal certainty with regards to virtual currencies slip by, at least in the field of anti-money laundering legislation. While the Fourth Anti-Money Laundering Directive will again address virtual currencies only incidentally, it leaves much space for Member States to carry out a risk assessment and gauge the risk that virtual currencies pose. While it seems likely that the opinion that virtual currencies are a high-risk vehicle will be prevalent,[67] some Member States, especially those with a large amount of online services businesses and virtual currency-related start-up businesses on their territory, might look upon virtual currencies more favourably.

The biggest and most pressing challenge faced by providers of mobile payments is not of a regulatory nature, but to exclude security risks regarding their users' financial information. Compared to virtual currency service providers, providers of mobile payment services seem to be well-equipped to meet the regulatory demands set to them, as they are clearly spelled out, and are drafted in such a way as to clearly apply also to mobile payments as well as non-mobile solutions.

This amount of legal certainty does not exist for virtual currencies. Businesses using a virtual currency environment, especially Bitcoin, have already learned to err on the side of caution and scrape along with the framework already in place with the Third Anti-Money Laundering Directive. Though a clearer framework was anticipated and desired, an incomplete framework like the present is still preferable to a heavy-handed regulation favoured by some parties, which has the potential to stifle innovation in the virtual currency business and which would most severely affect those businesses which wish to play by the rules, while having little or no effect on the illegal services and market places already operating on the network.

Lastly, to end on a positive note, although the European lawmaker is not including any specific measures relating to virtual currencies, all Member States are now prompted to review their national anti-money laundering legislation. It is to be hoped that while amending their national laws to implement the directive, Member States will take the

[67] FATF, Guidance for a risk-based approach, 31 f.

chance to create that oft-mentioned legal certainty on a national level, and create a clear legal framework for the implementation of anti-money laundering measures on virtual currencies, thereby encouraging innovation in this field in Europe.[68]

References

Cuéllar, M.-F. (2003). The tenuous relationship between the fight against money laundering and the disruption of criminal finance. Journal of Criminal Law and Criminology, 93, 311–465, 2003; Available at SSRN: http://ssrn.com/abstract=354740. Accessed 15 Aug. 2015.

European Banking Authority (EBA). (2015). *EBA opinion on virtual currencies*. https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf. Accessed 13 Oct. 2015.

European Central Bank. (2015). *Virtual currency schemes – A further analysis*. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf. Accessed 20 Aug. 2015.

European Commission. (2013). *Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*. COM(2013)45 final.

Eurofinas. (2015). *Eurofinas Observations on the Commission's Proposal for a Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*. COM(2013) 45 final http://www.eurofinas.org/uploads/documents/positions/AML/Eurofinas observations-final.pdf. Accessed 15 Oct. 2015.

European Payments Council (EPC). *Overview mobile payments initiatives*. EPC091-14, Version 2.0.

Europol. (2015). *The Internet Organized Crime Threat Assessment (IOCTA)*.

Financial Action Task Force (FATF). (2015). *Money laundering using new payment methods*. http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf. Accessed 13 Oct. 2015.

[68] The individual regulatory approaches of several countries within and outside of Europe are summarized in FATF (2015), p. 15 ff.

Financial Action Task Force (FATF). (2015). *International standards on combating money laundering and the financing of terrorism & proliferation* ("The FATF Recommendations")'. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf. Accessed 15 Aug. 2015

Financial Action Task Force (FATF). (2015). *Guidance for a risk-based approach – Virtual currencies*. http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. Accessed 15 Aug. 2015.

Grinberg, R. (2011). Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal, 4*, 159–208.

Gup, B. E. (2014). *What is money? From commodities to virtual currencies/Bitcoin*. http://ssrn.com/abstract=2409172. Accessed 15 Aug. 2015.

Luther, W. J. (2015). *Regulating Bitcoin: On what grounds?*. Available at SSRN: http://ssrn.com/abstract=2631307. Accessed 20 Aug. 2015.

Mitsilegas, V., & Gilmore, B. (2007). The EU legislative framework against money laundering and terrorist finance: A critical analysis in the light of evolving global standards. *International & Comparative Law Quarterly, 56*(1), 119–140.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf. Accessed 20 Aug. 2015.

Valant, J. & European Parliamentary Research Service. (2015, June) *Consumer protection aspects of mobile payments*. European Parliament Briefing. http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564354/EPRS_BRI%282015%29564354_EN.pdf. Accessed 12 Oct. 2015.

Valcke, P., Vandezande, N., & Van de Velde, N. (2015). *The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4*. Swift Institute Working Paper No. 2015–001. http://www.swiftinstitute.org/wp-content/uploads/2015/09/SIWP-No-2015-001-AML-Risks-of-the-Third-Party-Payment-Providers_FINAL.pdf. Accessed 13 Oct. 2015.

10

Virtual Currencies, M-Payments and VAT: Ready for the Future?

Redmar A. Wolf

Abstract VAT is a critical factor for the success of Bitcoin and other virtual currencies. The EU Court of Justice has recently decided that bitcoins should be treated as regular money, at least for purposes of VAT. The author addresses the implications of this decision and considers which VAT related questions are still left outstanding for Bitcoin. He concludes with some remarks about the VAT aspects of m-payments.

Developments in the area of law often fail to keep pace with technological advancements. A recent example of regulators lagging behind technological developments can be found in the appearance of virtual currencies with bitcoin as their most prominent representative and the use of mobile payments (m-payments). From a VAT perspective the use of these instruments implies entering unregulated territory. Nonetheless VAT is a critical factor for the success of bitcoin and other virtual currencies. A payment with regular money falls outside the scope of VAT. Payments

R.A. Wolf (✉)
Senior Counsel, Baker & McKenzie Amsterdam, Professor of indirect taxes, Faculty of Law, VU University of Amsterdam, Netherlands

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_10

in any other form are in principle subject to VAT as a payment in kind. Divergent views have existed with respect to the VAT qualification of bitcoins. In its recent decision in the case *David Hedqvist*[1] the EU Court of Justice (ECJ) has, however, shed some light on this topic and harmonized the EU VAT treatment to some extent.

In this chapter the author provides an introduction to the phenomenon of Bitcoin followed by an overview of its VAT implications. The author concludes with addressing the VAT issues of m-payments.[2]

An Introduction to Bitcoin

Bitcoin is an open source, peer-to-peer digital currency. It relies on the principles of cryptography (communication that is secure from view of third parties) to validate transactions and govern the production of the currency itself.[3] It was developed by a programmer (or group of programmers) who used the pseudonym Satoshi Nakamoto and whose identity remains unclear. The unit of the network is bitcoin or BTC (or XBT), which many consider a currency or internet cash.[4] This digital currency does not have a physical form but exists only as a balance on a bitcoin account (or "wallet").

Bitcoins are not issued by a state, bank or other financial institution, but are generated by the Bitcoin software itself and can only exist within that software. Bitcoins are not pegged to any real-world currency. The exchange rate is determined by supply and demand in the market. There are several exchange platforms for buying and selling bitcoins that operate in real time.[5]

[1] ECJ 22 October 2015, Case C-264/14, Skatteverket v David Hedqvist, ECLI:EU:C:2015:718.

[2] Reference is made to Bitcoin, capitalized, for the system (the software and the network it runs on) and bitcoin, lowercase, for the currency itself.

[3] Craig Kent Elwell, Maureen Murphy, Michael V Seitzinger, Bitcoin: Questions, Answers and Analysis of Legal Issues, Washington, Congressional Research Service, 20 December 2010, p. 1.

[4] Goldman Sachs, Global Market Research, Top of Mind, 11 March 2014, All about Bitcoin.

[5] An overview of such exchanges can be found at: http://bitcoincharts.com/markets/currency/EUR.html.

Nowadays, bitcoins are more and more accepted as tender.[6] Bitcoin offers users the advantages of lower transaction costs and increased privacy. However, there are also a number of disadvantages that could hinder wider use. These include sizable volatility of the price of bitcoins, and uncertain security from theft and fraud.

It is generally acknowledged that the Bitcoin technology is revolutionary and holds promise for a variety of alternative uses. In this chapter I will, however, only address the use of bitcoins as a means of payment. More specifically, I will only address the VAT consequences of such use.

Currencies, Money and Bitcoins

Throughout history, people have used a variety of currencies as means of payment. In this respect, a currency is something that goes round; something that is accepted in exchange for goods or services, not for itself but to be exchanged later for another good or service. A currency is a unit to quantify money. Money itself is, according to its intrinsic nature, abstract purchasing power.[7]

The first currencies were commodities with an intrinsic value such as livestock, seeds, gold and silver. Less valuable commodities were also used such as cowry shells or beads. These currencies were gradually replaced by coins and paper money. Commodity-backed money appeared, which consisted of items representing the underlying commodity (for instance: gold certificates).[8]

For a long time, currencies were privately issued; governments did not claim a formal monopoly over the issue and use of money within their territories.[9] As of the nineteenth century, monetary instruments were standardized and the status of legal tender was reserved for national currency. Another development was that commodity-backed money was replaced by fiduciary money. Such "fiat" money could no longer be redeemed for

[6] European Central Bank (October 2012), Virtual Currency Schemes, October 2012.

[7] Francis Mann, The Legal Aspect of Money, Oxford: At the Clarendon Press (1971), p. 29.

[8] European Central Bank (October 2012), Virtual Currency Schemes, p. 9.

[9] Aleksandra Bal, Stateless Virtual Money in the Tax System, European Taxation, July 2013.

a commodity. It is money issued by a central authority. People are willing to accept the money in exchange for goods and services simply because they trust this central authority.[10] Trust ("fiducia") is crucial for this kind of money. If the public loses its trust in the central authority, the money will lose its value.

With the creation of the World Wide Web and the ongoing proliferation of the internet, virtual communities appeared some of which issued their own virtual currencies. In this respect a digital currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community.[11] Bitcoin also falls within the latter category.

An Introduction to EU VAT

VAT, short for value added tax, is a primary source of income for many countries. Especially for EU countries, as they levy a VAT based on the framework set out in the VAT Directive.[12]This taxation applies generally to transactions relating to goods or services and is proportional to the price charged by the taxable person in return for the goods and services which he has supplied. The tax is charged at each stage of the production and distribution process, including that of retail sale, irrespective of the number of transactions which have previously taken place. The amounts paid during the preceding stages of the process are deducted from the tax payable by a taxable person, with the result that the tax applies, at any given stage, only to the value added at that stage and the final burden of the tax rests ultimately on the consumer.

The EU harmonization of VAT was set in motion because of two reasons. First of all, harmonization was needed to pave the way for a European single market. Back in 1967, Member States of the EEC[13]

[10] European Central Bank (October 2012), Virtual Currency Schemes, p. 10.

[11] European Central Bank (October 2012), Virtual Currency Schemes, p. 13.

[12] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax. O.J. 2006, L 347.

[13] The European Economic Community is more or less the predecessor of the EU. When the European Union (EU) was created in 1993, the EEC was transformed into the European

levied a variety of turnover taxes. These differences in taxation hampered intracommunity trade. To resolve this, the First[14] and Second[15] Directives, both enacted in 1967, obliged Member States to replace their existing turnover taxes with a VAT. The directives provided only a general outline of the VAT that the EU countries must introduce on their territory. Under the VAT regime (local) VAT was due on importation of goods, while VAT was paid back on export. This implied an equal tax burden for foreign and local products and created a level playing field for intracommunity trade.

The second reason for the VAT EU harmonization lies in the financing of Europe. In 1970[16] the European Council agreed that the European Communities should have "own resources". One of these own resources was (and is) the VAT resource, a certain percentage of the aggregate national VAT base that each country must pay to Brussels. The Sixth Directive[17] was adopted in 1977 to ensure that all Member States used the same set of rules to calculate their VAT base.[18] This directive has been replaced by the current VAT Directive.[19]

A taxable person performing VAT taxed activities must charge VAT on its output while claiming back the VAT paid on costs. As a result of this "taxation of output/deduction of input", a taxable person remits the VAT on the value it has added. Payment of VAT is thus divided between the various parties in the chain from producer to consumer. It is generally

---

Community (or EC), one of the EU"s three pillars (the other two were: the Common Foreign and Security Policy (CFSP) and Justice and Home Affairs (JHA), which was shrunk and renamed Police and Judicial Co-operation in Criminal Matters (PJC) in 2003). As of 1 December 2009 the Treaty of Lisbon made an end to the EU-pillar system; merging the EC with the other two pillars in a supranational system under the EU name.

[14] Directive 67/227 of 11 April 1967, O.J. No. 71, repealed by Directive 2006/112/EC.

[15] Directive 67/228 of 11 April 1967, O.J. No. 71.

[16] Decision of 21 April 1970 on the replacement of financial contributions from Member States by the Communities" own resources, O.J. No. L 94, 28.4.1970, p. 19.

[17] Sixth Council Directive 77/388/EEC of 17 May 1977, O.J. No. L 145 of 13 June 1977, p. 1, replaced by Council Directive 2006/112/EC (the VAT Directive).

[18] We see this reflected in the full name of this directive: "Sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonization of the laws of the Member States relating to turnover taxes – Common system of value added tax: uniform basis of assessment".

[19] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax.

believed that this system of fractioned payments makes VAT less susceptible to fraud than other forms of indirect taxation.

Money, Payments and VAT

One of the inherent features of the EU VAT system is that the mere payment of money does not in itself constitute a VAT taxable event. Although this feature is generally acknowledged, it is not specifically codified. It seems to follow from the structure of VAT as set forth in the VAT Directive. According to Article 2(2) of this directive, VAT is intended as a general tax on consumption exactly proportional to the price of the goods and services. One could imagine the consumption of coins or bills, for instance to create works of art or as (costly) fuel. However, generally speaking, money in its capacity as a means of payment cannot be consumed,[20] but only spent. Without consumption, there can be no taxation.

The ECJ recognized this principle in its decision in the case *Mirror Group* where the ECJ stated: "As to whether a supply of services was made, it must be noted that a taxable person who only pays the consideration in cash due in respect of a supply of services, or who undertakes to do so, does not himself make a supply of services for the purposes of Article 2(1) of the Sixth Directive."[21]

On the same date the ECJ also issued its decision in the case *Fitzgerald*. Here the ECJ held that: It is supplies of goods or services which are subject to VAT, rather than payments made by way of consideration for such supplies.[22]

The ECJ reiterated this point of view in *BUPA*: "In that connection, it must also be borne in mind that it is the supplies of goods or services which are subject to VAT, rather than payments made by way of consideration for such supplies (…)".[23]

---

[20] One could describe consumption as the process in which the recipient of goods or services changes these goods and services into something else.

[21] ECJ 9 October 2001, Case C-409/98, *Mirror Group*, ECLI:EU:C:2001:524, paragraph 26.

[22] ECJ 9 October 2001, Case C-108/99, *Cantor Fitzgerald*, ECLI:EU:C:2001:526, paragraph 17.

[23] ECJ 21 February 2006, Case C-419/02, *BUPA Hospitals and Goldsborough Developments*, ECLI:EU:C:2006:122.

The ECJ did not provide any indication that the above reasoning was limited to specific forms of "payments" such as currencies recognized as legal tender.

From the above it follows that a mere exchange of means of payment (where one supply of money is paid with a corresponding supply of money) does not fall within the scope of EU VAT. A reciprocal payment, where money in one form (or denomination) is traded in for money in a different form, thus remains outside the scope of VAT. That is, in as far as the value of the money traded in equals the value of the money received. A difference in values implies that one party does not only receive the monetary equivalent of the money traded in, but also an additional payment. This additional payment can be seen as a remuneration for the exchange itself.

This reasoning clearly underlies the judgment of the ECJ in the case *First National Bank of Chicago*.[24] This case addressed the VAT aspects of currency transactions of a bank. National currency was exchanged for foreign currency and vice versa using different exchange rates; an "offer" and a "bid" price. The "offer" rate was used when selling foreign currency, the "bid" rate was used when purchasing foreign currency (and, from a VAT point of view supplying national currency while receiving foreign currency as payment). The difference between the "offer" and the "bid" prices was known as "the spread". In its decision the ECJ held that this "spread" was in fact the remuneration the bank received for the exchange of currency. The exchange of the currencies itself was disregarded.

In its written observation in this case the UK Government considered that in the absence of consideration, a foreign exchange transaction entered into without the charging of a commission or a fee did not constitute a supply of goods or services but was simply the exchange of one means of payment for another. With respect to the mere exchange of one means of payment against another means of payment, the ECJ implicitly followed the UK observations; such exchange did not in itself constitute a VAT relevant event. However, the ECJ found that the use of offer and bid prices and the ensuing "spread" did in fact constitute remuneration for the exchange transactions.

[24] ECJ 14 July 1998, Case C-172/96, *First National Bank of Chicago*, ECLI:EU:C:1998:354.

More recently Advocate General Kokott addressed this issue in her conclusion in the case *Granton Advertising*.[25] Here Kokott stated that:

> 41. Such an approach is also consistent with the objectives which I attribute to the exemption of transactions concerning negotiable instruments. In my view, such instruments are rights which are regarded in the course of trade as being similar to money and which are to be treated for VAT purposes in the same way as payments of money. Payments of money are admittedly not taxed as such, but are rather simply the consideration for a taxed supply, either because they are neither a supply of goods nor a supply of services within the meaning of Article 2(1) of the Sixth Directive, (21) or because they are non-taxable by virtue of Article 13(B)(d)(4) of the Sixth Directive.

Kokott holds that "rights" with the same use as money should also be treated as money for purposes of VAT. The transfer of such rights should be treated as the mere transfer of money, a payment, and therefore remain outside the scope of VAT. The ECJ did not specifically address this issue in its decision in this case as it explicitly found in its "preliminary remarks" that contrary to what was indicated by the referring court,[26] the use of a Granton card could not be considered a "payment" for the purpose of the Sixth Directive. Based on this finding, the ECJ concluded that the issuance of the Granton card was taxed.[27] Clearly, the VAT consequences would have been different had the Granton card been qualified as a means of payment.

Paying with Bitcoins

When looking at the VAT aspects of bitcoins, the first question that comes to mind is whether bitcoins should be treated as a means of payment comparable to other sorts of money. If you pay with bitcoins, should this

[25] Conclusion of Advocate General J. Kokott of 24 October 2013, Case C-461/12, *Granton Advertising BV*, ECLI:EU:C:2013:700.

[26] The Dutch District Court (Gerechtshof) of Den Bosch.

[27] ECJ 12 June 2014, Case C-461/12, *Granton Advertising BV*, ECLI:EU:C:2014:1745.

supply be treated the same as the supply of regular money—and thus remain outside the scope of VAT—or does this supply constitute a payment in kind? In the latter case bitcoin users may be obliged to pay VAT on their spending of bitcoin.

In what is considered the first landmark case (2013) involving bitcoins the US Magistrate Judge Amos Mazzant claimed that Bitcoin is a form of money:

> It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and (…) used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or form of money (…).[28]

Other parties in the USA did not agree with the qualification of bitcoins as money. In 2014 the US Internal Revenue Service issued guidelines on the tax treatment of virtual currencies. According to this "Notice 2014–21" virtual currencies, including bitcoins, qualify as tangible personal assets. As a result, bitcoins are an investment subject to capital gains. Bitcoins will also be taxed with income tax if used to pay for goods and services.[29] In 2015 another US institution, the US Commodities Futures Trading Commission, took the position that bitcoins and other virtual currencies were a commodity covered by the Commodity Exchange Act.[30]

Across the ocean in the EU, virtual currencies such as bitcoins also received a mixed legal reception. Especially when it related to VAT. In

[28] Memorandum opinion regarding the Courts subject matter jurisdiction (6 August 2013, Judge Amos Mazzant), *US Securities and Exchange Commission v. Trendon T. Shavers et al.*, case number 4:13-cv-00,416, in the US District Court for the Eastern District of Texas.

[29] See: IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for US Federal Tax Purposes; General Rules for Property Transactions Apply, https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance (accessed 18 November 2015).

[30] CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering, http://www.cftc.gov/PressRoom/PressReleases/pr7231-15 (accessed 18 November 2015).

the UK the tax authorities[31] advocated the view that bitcoins were money for purposes of VAT. This implied that supplying bitcoins as payment was not a payment in kind, but fell outside the scope of VAT. On the other hand, the German Federal Ministry of Finance[32] and the Austrian Ministry of Finance[33] took the position that bitcoins did not qualify as money. In their view, paying with bitcoins constituted a payment in kind for purposes of VAT. The supply of bitcoins entails the transfer of the entitlement to certain rights in a separate network. Such a supply does not fall under any of the current exemptions in the VAT Directive and will therefore be subject to VAT when performed by a tax payer. Under this scenario anyone paying with bitcoins on a regular basis, and thus supplying services on a regular basis, becomes a VAT taxable person. The mere spending of bitcoins would then attract an obligation to pay VAT. Traders accepting bitcoins as payment will be confronted with an additional VAT levy when they exchange bitcoins for regular currencies. Also, should the trade in bitcoins be VAT taxed, such market may offer a breeding ground for carousel fraud.[34]

The recent decision of the ECJ in the case *David Hedqvist*[35] put an end to the above divergent VAT treatment of bitcoins.

The Case of David Hedqvist

David Hedqvist was a Swedish individual who was planning to offer bitcoin exchange services. Hedqvist had received a ruling from the Swedish Authority for the Ruling (Skatterättsnämnd) stating that these activi-

[31] This approach was put forward in: Revenue & Customs Brief 09/14, Tax treatment of activities involving Bitcoin and other similar cryptocurrencies, issued 3 March 2014, http://www.hmrc.gov.uk/briefs/vat/brief0914.htm (accessed on 18 November 2015).

[32] In a letter dated 24 April 2014 from Dr. Michael Meister (Parlamentarischer Staatssekretär beim Bundesminister der Finanzen) on: Umsatzsteuerliche Behandlung von Bitcoins, see also: http://www.bundesverband-bitcoin.de/wp-content/uploads/2014/05/140512-Antwort-PStS-Meister.pdf (accessed on 18 November 2015).

[33] Letter from Bundesminister Dr. Michael Spindelegger to the Austrian Parliament dated 22 July 2014, GZ. BMF-310,205/0115-I/4/2014.

[34] By using the same mechanisms that were previously used in the trade of carbon rights, see: Redmar Wolf, The Sad History of Carbon Carousels. VAT Monitor 2010, no. 6.

[35] ECJ 22 October 2015, Case C-264/14, *Skatteverket v David Hedqvist*, ECLI:EU:C:2015:718.

ties would be VAT exempt. According to the Skatterättsnämnd bitcoins should be considered "currency" for purposes of VAT, and reference was also made to the decision of the ECJ in the case *First National Bank of Chicago*.[36] The Swedish tax authority (Skatteverket), however, appealed against the decision Skatterättsnämnd. Legal proceedings followed in which the Swedish Supreme Court found that the decision of the ECJ in the case *First National Bank of Chicago* did not necessarily relate to virtual currencies like bitcoin. The court decided to stay the proceeding and referred the following questions to the ECJ:

> Is Article 2(1) of the VAT Directive to be interpreted as meaning that transactions in the form of what has been designated as the exchange of virtual currency for traditional currency and vice versa, which is effected for consideration added by the supplier when the exchange rates are determined, constitute the supply of a service effected for consideration? If the answer to the first question is in the affirmative, is Article 135(1) to be interpreted as meaning that the abovementioned exchange transactions are tax exempt?[37]

In answering these questions, Advocate General Kokott and the ECJ addressed some fundamental VAT issues of Bitcoin.

First of all, the question of whether paying with bitcoins constitutes a VAT taxable event. In her opinion, Advocate General Kokott refers to the *First National Bank of Chicago* where the ECJ held that the exchange of currencies in relation to which a bank sets different rates for the sale and purchase of the currencies involved constitutes the supply of a service effected for consideration. In this respect Kokott notes:

> 13. (…) However, the taxable service effected by the bank comprised the exchange activity only, and not the transfer of the currencies themselves. The Court of Justice considered that this transfer constituted neither a supply of goods nor a supply of services, as the currencies were legal tender. (4) The court found that in principle the consideration for the taxable exchange

[36] ECJ 14 July 1998, Case C-172/96, *First National Bank of Chicago*, ECLI:EU:C:1998:354.

[37] Request for a preliminary ruling from the Högsta förvaltningsdomstolen (Sweden) lodged on 2 June 2014 — Skatteverket v David Hedqvist (Case C-264/14).

service consisted in the difference between the purchase and sale prices for the currencies.

14. The judgment was based on the fact that the transfer of legal tender as such is accepted as not constituting a chargeable event for VAT purposes. (…) Rather, such a transfer can in principle (…) only constitute the consideration for a taxed supply, as VAT is a tax on the end consumption of goods. (…) Currencies currently used as legal tender — unlike gold or cigarettes, for instance, which also are or have been used directly or indirectly as means of payment — have no other practical use than as a means of payment. Their function in a transaction is simply to facilitate trade in goods in an economy; as such, however, they are not consumed or used as goods.

15. That which applies for legal tender should also apply for other means of payment with no other function than to serve as such. Even though such pure means of payment are not guaranteed and supervised by law, for VAT purposes they perform the same function as legal tender and as such must, in accordance with the principle of fiscal neutrality in the form of the principle of equal treatment, (…) be treated in the same way.

16. This is consistent with the case-law. The case-law treats legal tender and other pure means of payment — such as vouchers with a face value (…) or the purchase of "points rights" for later use in hotels or accommodation (…) — in largely (…) the same way, in that in the latter cases the transfer of the means of payment is not held to constitute a taxable transaction.

17. According to the findings of the referring court, bitcoins also constitute a pure means of payment. The only purpose of possessing them is to reuse them as a means of payment at some point. For the purposes of the chargeable event for VAT, therefore, they must be treated in the same way as legal tender.[38]

Kokott concludes that the approach in *First National Bank of Chicago* must also be applied to bitcoins. Their transfer as such does not constitute a chargeable event. However, as Mr. Hedqvist plans to buy and sell bitcoins for Swedish crowns at a price which includes a markup on the

[38] Opinion of Advocate General Kokott, delivered on 16 July 2015, Case C–264/14, *Skatteverket v David Hedqvist*, ECLI:EU:C:2015:498.

exchange rate on a particular exchange site, his activity includes VAT relevant services in the form of the exchange.

In its decision the ECJ characterizes bitcoins as virtual currency with bidirectional flow. This virtual currency has no purpose other than to be a means of payment. Like means of payment officially recognized as "legal tender" (the ECJ refers to "traditional currencies"), bitcoin cannot be considered tangible property.[39] According to the ECJ, the exchange of different means of payment, does not qualify as a VAT relevant "supply of goods". However, the exchange at hand constitutes a VAT relevant service. The remuneration for this service is the margin that Hedqvist includes in the calculation of the exchange rate at which he is willing to sell and purchase the currencies concerned.

The ECJ thus follows in *David Hedqvist* the same reasoning as in *First National Bank of Chicago*. The respective supplies of means of payment (whether or not qualifying as legal tender) are disregarded. Relevant is only the exchange of means of payment in as far a spread is realized on this exchange. Apparently, paying with bitcoin is put on the same footing as paying with legal tender; this "supply" falls outside the scope of VAT.

The Exchange Service: Exempt?

Once it is established that the exchange of bitcoin against a regular currency constitutes a VAT relevant service, the question arises whether this service is taxed or exempt.

Also on this issue differing opinion existed between the Member States. UK tax authorities suggested an exemption: "Charges (in whatever form) made over and above the value of the Bitcoin for arranging or carrying out any transactions in Bitcoin will be exempt from VAT under Article 135(1)(d) [of the VAT Directive]."[40]

Other EU countries advocated a different approach; Austria, for instance, was of the opinion that: "Der Umtausch von virtuellen Währungen in

[39] In the French version of the decision bitcoin is described as: "moyens de paiement" while legal tender is: "moyens de paiement légaux". See: Redmar Wolf, Bitcoin and EU VAT. International VAT Monitor, October/September 2014, p. 254.

[40] Revenue & Customs Brief 09/14, paragraph 4.

gesetzliche Zahlungsmittel kann einen steuerbaren und steuerpflichtigen Umsatz darstellen, wenn der Umtauschende Unternehmer ist, der diesen Umsatz im Rahmen seines Unternehmens ausführt."[41]

In *David Hedqvist* the ECJ decides this matter; the exchange services are VAT exempt, although not under the provision suggested by the UK tax authorities (Article 135(1)(d) of the VAT Directive). The latter provision refers to transactions relating to, *inter alia*, "deposit and current accounts, payments, transfers, debts, cheques and other negotiable instruments". According to the ECJ this means that services or instruments must be involved that operate as a way of transferring money. The exemption thus concerns only derivatives of currency and not the currencies themselves.

According to the ECJ the "bitcoin" virtual currency, is not a current account or a deposit account, a payment or a transfer but, instead, a direct means of payment between the operators that accept it. As a result, Article 135(1)(d) of the VAT Directive does not apply to the exchange of bitcoins.

The ECJ subsequently reviews the exemption for transactions involving, *inter alia*, "currency" [and] bank notes and coins used as legal tender (Article 135(1)(e) of the VAT Directive). From the various language of this provision it is not clear whether this exemption is restricted to transactions involving traditional currencies (legal tender) or also encompasses transactions involving other currencies. Where there are linguistic differences in the various versions of a provision, the context of the provision and the aims and scope of the VAT Directive must be taken into account for determining the scope of the provision.

The exemption for transactions involving currency is intended to alleviate the difficulties connected with determining the taxable amount and the amount of VAT deductible which arise in the context of financial transactions. Such difficulties not only exist when traditional currencies are exchanged but also when traditional currencies are exchanged for virtual currencies which are accepted as means of payment. Transaction in non-traditional currencies, such as bitcoin, are financial transactions.

[41] Letter from Bundesminister Dr. Michael Spindelegger to the Austrian Parliament dated 22 July 2014, GZ. BMF-310,205/0115-I/4/2014, paragraph 19.

Limiting the scope of the exemption to transactions involving only traditional currencies would then deprive the exemption of part of its effect. From this the ECJ concludes that the exemption for transactions in currencies should also cover the exchange of bitcoins at hand.

Exchanging bitcoins for legal traditional currencies is thus put on the same footing as the "regular" exchange of traditional currencies.

Defining Bitcoin

The decision of the ECJ in *David Hedqvist* includes a description of bitcoin and its peculiarities. In this respect the ECJ does not refer to legislation, but to "common ground". According to the ECJ it is common ground that the bitcoin virtual currency has no other purpose than to be means of payment and that it is accepted for that purpose by certain operators. It is also common ground that the bitcoin is neither a security conferring a property right nor a security of a comparable nature.[42] The ECJ refers to bitcoin as being a virtual currency with bidirectional flow. The ECJ also notes that the bitcoin virtual currency cannot be regarded as "tangible property" nor as a current account, a deposit account, a payment or a transfer.

Accepting Bitcoins as Payment

In *David Hedqvist* not all VAT aspects of the use of bitcoins were addressed. The ECJ did not provide guidance on the valuation of bitcoins. When a retailer accepts bitcoins as a remuneration for taxed goods or services, VAT will be due on the value of the bitcoins. This matter is undisputed; paying with bitcoins does not imply that goods or services acquired with bitcoins become VAT free. The practical issue here is, however, how the taxable amount should be calculated when receiving bitcoins as payment. Which exchange rate should be used? Article 91(2) of the VAT Directive prescribes that when accepting a currency other

[42] As mentioned in Article 135(1)(f) of the VAT Directive.

than that of the EU country where the taxable transaction takes place, "the exchange rate applicable shall be the latest selling rate recorded, at the time VAT becomes chargeable, on the most representative exchange market or markets of the Member State concerned, or a rate determined by reference to that or those markets, in accordance with the rules laid down by that Member State."

The question that arises here is whether bitcoin qualifies as a "currency" as mentioned in this provision. This term seems restricted to "legal tender", something bitcoin clearly is not. Following the reasoning that the ECJ applied with respect to the scope of the exemption for transactions in (virtual) currencies, however, Article 91(2) of the VAT Directive should also apply to bitcoin transactions. Exchange rates for bitcoins are readily available on the internet, although it is not clear how the "most representative" market should be determined.[43]

Creating Bitcoins Through Mining

Another issue that the ECJ did not address was the VAT treatment of bitcoin mining. Bitcoin mining is the process of making computer hardware do mathematical calculations for the Bitcoin network to confirm transactions and increase security. It involves applying computer power to solve complicated algorithms. Once such math problem is solved ("a new block is mined") the network itself awards a certain amount of newly generated bitcoins to the miner.

In my view obtaining bitcoins through the process of mining does not constitute a VAT relevant activity. The bitcoins are automatically generated by the network itself; there is no specific customer for the mining activities. Mining therefore does not lead to a situation in which a legal relationship exists between a provider of a service and the recipient (the customer) as the ECJ described in its decision in the case *Tolsma*.[44] Without such legal relationship, there is no supply against consideration and no VAT taxable event.

[43] See for instance: http://www.coindesk.com/price/.

[44] ECJ 3 March 1994, Case 16/93, *R. J. Tolsma v Inspecteur der Omzetbelasting Leeuwarden*.

If the miner subsequently exchanges the bitcoins against regular currency, goods or services this does not constitute a taxable event either. As can be derived from *David Hedqvist* the supply of bitcoins is a mere payment and falls outside the scope of VAT.

The process of mining may also involve validating payments. A bitcoin transaction will only be processed in the Bitcoin network when it is validated by a miner. A party who wants to transfer bitcoins may include a transaction fee in its payment order. Miners are then enticed to process this transaction with priority.

The party placing the payment order does not know which miner will process the transaction, nor does the party placing the payment order have any recourse against this miner if anything goes wrong. A legal obligation to pay a transaction fee does not exist; miners are not entitled to transaction fees. Transaction fees can be compared with a tip or gratuity left for the miner. For VAT purposes, transaction fees will likely not qualify as a remuneration for the processing of the payment. As a result, this mining activity will also remain outside the scope of VAT.

However, let us assume that the transaction fees *does* constitute a VAT relevant remuneration for the processing activity. The question then arises whether this processing is taxed or exempt. In my view, these activities will likely fall under the exemption for transactions concerning payments (Article 135 (1)(d) of the VAT Directive). In its decision in the case *SDC*[45] the ECJ held that such transactions must have the effect of transferring funds and entail changes in the legal and financial situation. The validating activities of miners seem to do just that.[46]

Outside the scope of VAT or VAT exempt, in any event miners will likely not perform VAT taxed activities. However, as these activities comprise "breaking new ground", it may be expected that the ECJ will be asked to shed its light on the VAT implications of bitcoin miners in due course.

[45] ECJ 5 June 1997, Case C-2/95, *Sparekassernes Datacenter* (*SDC*), paragraph 66.

[46] This view is advocated by the UK tax authorities Revenue & Customs Brief 09/14, paragraph 2.

Conclusions for Bitcoin

Bitcoin offers an alternative means of payment. In its decision in *David Hedqvist* the ECJ has confirmed that for purposes of VAT the use of bitcoins is treated as the use of any other means of payment. This implies that paying with bitcoins constitutes a mere payment and is not a relevant transaction for VAT purposes. When receiving bitcoins as payment, VAT will be due on the value using exchange rates which are readily available on the internet. Exchanging bitcoins for regular currencies remains outside the scope of VAT. Any commission received in this respect is VAT exempt.

The activities of bitcoin miners were not covered by the decision of the ECJ in *David Hedqvist*. It is likely that these activities will not attract VAT. However, the ECJ will have the final say in this matter. Preliminary questions on this were not referred yet, but I expect such questions will follow in due course.

All in all, despite its revolutionary nature, Bitcoin does not attract too many VAT complications within the EU. This is because the ECJ has put the use of bitcoins on the same footing as the use of regular currencies. As a result, from a VAT perspective, the EU is ready for the future of this new form of payment.

VAT and M-Payments

Compared to bitcoins, the VAT issues for m-payments are rather straightforward. M-payments normally relate to legal tender. As a result, the VAT consequences of this new type of payment do not differ from other ways through which entitlement to regular currency is transferred. Such transfer itself, the payment, falls outside the scope of VAT. Receipt of money through this medium may constitute a payment for goods and services and thus attract VAT.

When mobile phone services enable subscribers to send money, there is a combination of a telecommunication service and a financial service. The various parties involved in arranging this transaction will normally receive a fee. Here VAT complications may occur.

Pursuant to Article 135(1)(d) of the VAT Directive an exemption applies to "transactions concerning transfers and payments". Although this exemption was originally intended for payment services rendered by financial institutions, it is clear from the ECJ"s judgment in SDC[47] that it also applies to such services supplied by other service providers. In the same decision the ECJ held that the exemption thus applied to services which have the effect of transferring funds and entail changes in the legal and financial situation of the parties involved. That certainly happens when using m-payments. However, when several parties are working together to complete payments it may be unclear whose services are VAT exempt and whose services are VAT taxed (for instance because they concern telecommunication services which are not exempt). It all depends on the legal (and factual) relationships between parties. In any event, facilitators of m-payments should not disregard VAT when starting up their activities.

References

Bal, A. (2013, July). Stateless virtual money in the tax system. *European Taxation*. 53 (7), 351–356.

Elwell, C. K., Murphy, M. M., & Seitzinger, M. V. (2013). *Bitcoin: Questions, answers and analysis of legal issues*. Washington, DC: Congressional Research Service.

Mann, F. (1971). *The legal aspect of money*. Oxford: At the Clarendon Press.

Wolf, R. (2010). The sad history of carbon carousels. *VAT Monitor, 6*, 10–17.

Wolf, R. (2014). Bitcoin and the EU VAT. *International VAT Monitor*. September/October. 254–257.

[47] ECJ 5 June 1997, Case C-2/95, *Sparekassernes Datacenter* (*SDC*).

11

Mobile Payments and Merger Regulation: A Case Law Analysis

Daniele D'Alvia

Abstract D'Alvia offers an updated overview of the main competition issues that currently affect the m-payment ecosystem through a case law analysis of two recent decisions upheld by the European Commission. M-payment solutions are still in their infancy and are the product of fast technological improvements. Hence, the chapter is aiming at the examination of preliminary operative aspects of joint ventures that are created by banks and mobile network operators in order to prevent the occurrence of possible anticompetitive effects of such cooperation in terms of vertical, horizontal and conglomerate merger effects.

This chapter explores the mobile network based payment systems (m-payment) from a competition law perspective. Following an illustration of two recent competition cases, the attention is focused on the main aspects and issues to be monitored by competition authorities and regulators in order to avoid and mitigate possible anticompetitive behaviors in relation to joint ventures operating in the mobile commerce industry.

D. D'Alvia (✉)
Birkbeck University of London, UK

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_11

JV Telefónica, CaixaBank and Banco Santander (Case No. COMP/M. 6956)

On 14 August 2013, the European Commission cleared the creation of a joint venture between Telefónica SA (Telefónica),[1] CaixaBank SA (CaixaBank),[2] and Banco Santander SA (Banco Santander).[3]

The NewCo deriving from the notified transaction provides consumers and merchants in Spain, members of its "virtual community", with a number of retail services, accessible by both desktop and mobile channels.

As to consumer members of the virtual community, the NewCo provides a number of "digital wallet services".

Such services include a repository of payment methods, which allows consumers to upload the details of any credit, debit, or prepaid cards into the wallet functionality. Thus, consumers can use such uploaded information to pay online either remotely or in a store through a smartphone. Furthermore, the mobile wallets include an identification system (the existence of a client ID to identify the consumer in order to make the payment). By means of such ID, consumers are able to pay frictionless, while merchants are able to identify consumers in order to offer to them benefits and promotions.

Finally, ancillary peer-to-peer (P2P) payment services are provided. This is a functionality which allows consumers who are part of the virtual community to make payments between themselves.

As to merchant members of the virtual community, the NewCo provides two main services. These are the digital advertising services and the ancillary analytics services. The former enables merchants to advertise their products and make them accessible by consumers as well as to cre-

[1] The parent company of the Telefónica Group, an international telecommunication company providing communication, information and entertainment services in Spain, Germany, Ireland, the Czech Republic, Slovakia and the UK and in a number of countries in South America.

[2] A financial institution wholly controlled by La Caixa, Caja de Ahorros ("La Caixa"), the parent company of La Caixa Group, active in banking, insurance, pension and investment activities mainly in Spain and internationally by means of strategic alliances and a network of representative offices.

[3] The parent company of the Santander Group, active in banking, asset management, corporate and investment banking, treasury and insurance in Europe, South America, the USA and marginally in Asia.

ate new online and mobile based couponing and loyalty services, while the latter enables merchants to analyse consumers' habits and purchasing preferences, in order to personalize promotions, offers, vouchers and loyalty programmes.

Before assessing the possible horizontal, vertical and/or conglomerate effects that the joint venture might cause, the European Commission firstly starts to determine the relevant markets in order to establish consequently whether the undertakings involved in the joint venture could retain and exercise a dominant position in those specific markets, and, therefore, commit an abuse of that position in contrast to Article 102 of the Treaty on the Functioning of the European Union (TFEU).

The Definition of the Relevant Markets

The European Commission identifies the existence of seven relevant product markets potentially affected by the notified transaction, namely: the market for digital (online and mobile) advertising; the market for data analytics services; the market for retail distribution of digital wallet services; the market for payment card issuing; the merchant acquiring market; the market for the provision of retail mobile telephony services (including mobile data access); and the market for the retail provision of fixed broadband internet access.

All of these markets have been considered by the European Commission as national in their geographic scope.

Finally, it should be noted that according to the European Commission one of the relevant product markets, namely the merchant acquiring market is not taken into account for investigation purposes in the present case because the share that Banco Santander holds on this market and any of its possible subdivisions[4] is below 25 %.

[4] In particular the European Commission has in previous decisions (Commission decision of 3 October 2008 in Case COMP/M. 5241, Commission decision of 29 September 2006 in Case COMP/M. 4316, Commission decision of 2 June 2005 in Case COMP/M. 3740, Commission decision of 8 November 2001 in Case COMP/M. 2567) held that the merchant acquiring market may be further subdivided according to different parameters such as the type of scheme organization (international, domestic), customer type (consumer, commercial), type of card (debit, credit) or according to the brand (MasterCard, Maestro, American Express Personal Green Card, etc.).

Antitrust Regulatory Concerns on Horizontal Assessment

When assessing the possible horizontal effects,[5] which could be created by the NewCo on the identified relevant markets, the European Commission deemed as follows.

As to the market for digital (online and mobile) advertising services, the European Commission found that the concentration did not give rise to serious doubts as to its compatibility with the internal market, since only Telefónica offered advertising inventory (as online display format, banners on its mobile portals and advertising messaging sold by aggregators), but owned on this market only a very limited share. Moreover, the European Commission deemed that both the NewCo and Telefónica would continue to face competition from a number of well-established global players, such as Google and Yahoo.

As to the market for the retail distribution of digital wallet services, the European Commission excluded any competition concern since none of the notifying parties are active in the retail distribution of digital wallets in Spain, save from a minor presence of CaixaBank through its "CaixaWallet" product. In addition, the NewCo would anyway compete with a number of well-established players in the sector, both multinational (PayPal, Google, Apple, Visa, MasterCard, AmEx etc.) and startuppers active in Spain (MomoPocket, Kuapay, Payment etc.). In this regard, the market investigation confirmed that a number of digital wallet providers already exist or are very likely to emerge in Spain in the near future, ensuring that an effective competitive environment would continue to exist also after the creation of the NewCo.

Antitrust Regulatory Concerns on Non-Horizontal Assessment

Beside the horizontal aspect of the transaction, the European Commission assesses whether there is also a vertical and/or conglomerate competitive relationship between card payment services and the retail distribution of

[5] A merger has horizontal effects when undertakings are producing the same product and, therefore, are actual or potential competitors in the same relevant market.

digital wallet services, including the P2P payment services. Hence, the European Commission assesses whether the future merged entity, namely NewCo, could exercise a market power in terms of abuse of dominant position.

Firstly, there could be a vertical relationship between the issuing of (virtually prepaid) payment cards (where two of the NewCo's parents are active) and the provision of P2P payment services within the NewCo's digital wallet. Thus, there could be risks of input and customers foreclosure.

The European Commission considered that a risk of input foreclosure could be excluded in the present case, since in Spain there are sufficient credible alternative issuers of payment cards other than Banco Santander and CaixaBank, and the market is highly fragmented: hence, providers of competing digital wallets would anyway be in a position to partner, if necessary, with competing banks in order to integrate virtual payment cards into their digital wallet if it is needed to provide P2P services.

Furthermore, as to the risk of customer foreclosure for competing payment card issuers, the European Commission considered that it could be excluded in the present case. Indeed, such a risk would only arise if the NewCo opted to integrate virtual payment cards issued by one of its parents; the consumers of the virtual community would renounce to use other payment cards that they own and thereby competing issuers of payment cards would lose a significant amount of customers. Such concerns were excluded by the Commission in the present case given that the limited scope of the use of the payment card in the NewCo's digital wallet would have unlikely refrained a consumer to use the payment cards they already owned. Moreover, even if all of the customers of the NewCo would stop using their pre-existing cards, this would have a very limited impact on the market, as the number of customers of the NewCo is just small.

Secondly, there could be a conglomerate relationship between the issuing of payment cards and the provision of digital wallet services: given that a customer would need to upload his or her payment card details into the digital wallet in order to use the latter for online and m-payments to merchants of the virtual community, there is a complementary relation-

ship between the issuing of payment cards and the provisions of digital wallet services, which may potentially generate conglomerate effects.

In this regard, the European Commission deemed that there was no risk that the NewCo would foreclose neither the providers of competing digital wallets nor the providers of competing payment card issuers. Indeed, on the one hand, the European Commission found that CaixaBank and Banco Santander, due to their lack of significant market power and the fragmentation of the market, would not have the ability to foreclose competing digital wallets by restricting or totally blocking the use of payment card issued by them in such competing digital wallets. On the other hand, the European Commission noted that users of the NewCo would be able to upload any debit, credit or prepaid card into the digital wallet regardless of the relevant issuing bank, and they would be able to purchase products and services with any payment method, including physical payment in stores. Thus, the digital wallet would be more attractive should it accept all payment cards, as this was already allowed by the competing digital wallet already on the market.

Thirdly, there could be a conglomerate relationship between the provision of mobile telephony and internet access services provided by Telefónica on the one hand and the retail distribution of digital wallet services provided by the NewCo.

In this regard, the European Commission excluded the existence of both a risk of foreclosure of competing digital wallets and a risk of foreclosure of competing providers of retail mobile telephony services and fixed broadband internet access services. This was because the presence of a digital wallet on a mobile handset does not represent in the retail mobile telephony market an essential element in terms of changing and influencing the consumers' preference when they select a provider of mobile telephony.

The European Commission's Decision

The European Commission found that Telefónica, regardless of its quite considerable market position, would not be technically able to block or

restrict the use of competing digital wallets on its own mobile and fixed broadband internet networks, on the basis that:

- NewCo's digital wallet is not linked on an exclusive or preferential basis to Telefónica;
- digital wallet activities are usually not dependent on any broadband network, since the secure element (SE) is either placed on the cloud or is embedded on a specific device; that there are alternative methods of placing the SE other than on a subscriber identity module (SIM) card;
- digital wallets do not use any SIM; and that as long as the digital wallet app can be downloaded from any device, clients from any mobile operator will be able to download the digital wallet app irrespective of their phone operator.

Finally, the European Commission excluded the risk of foreclosure of competing providers of retail mobile telephony services and fixed broadband internet access services, since the digital wallet can be accessed via any mobile phone service providers and via any network of broadband internet connection. By contrast, the NewCo had a significant interest in making the digital wallet accessible by non-Telefónica customers in order to make it more attractive and profitable.

In light of the described competition assessment, the European Commission cleared the concentration and declared it compatible with the internal market and with the European Economic Area (EEA) agreement.

JV Telefónica UK, Vodafone UK, Everything Everywhere (COMP/M. 6314)

On 4 September 2012, the European Commission—following a Phase II investigation—unconditionally cleared a concentration whereby the three biggest mobile operators in the UK,[6] Telefónica UK Limited

[6] They accounted for 90.5 % of retail mobile revenuers in the UK at the time of the filing.

(Telefónica UK),[7] Vodafone Group Plc (Vodafone Group),[8] and Everything Everywhere Limited (Everything Everywhere)[9] (together, the Parent Companies) set up a joint venture, namely the JV Co, of which they have control within the meaning of Article 3(1)(b) of the Regulation (EC) No. 139/2004 (the Merger Regulation). The JV Co offers various mobile commerce services to businesses in the UK, encompassing m-payments, mobile advertising and data analytics.

The JV Co cleared by the European Commission provides businesses (including the Parent Companies and third-party mobile operators) with a variety of services, while no services are directly addressed to consumers.

In particular, the JV Co provides a wallet platform, which is a platform enabling the supply of transaction services accessible offline through a near field communication (NFC)[10] enabled mobile handset as well as online via the internet. The services supplied by the wallet platform are payment in shops, ticketing and access services as well as voucher and loyalty services, enabling the provision of digital vouchers to consumers (services); they are addressed to commercial entities, such as banks, other payment card issuers, loyalty card issuers, ticket issuers and other retailers (service providers).

Moreover, the JV Co provides mobile marketing services, so that a single point of contact is available for advertisers and media agencies who wish to develop advertising campaigns targeted at customers of mobile operators, whether through push messages, coupons and vouchers, or through the sale of advertising space.

---

[7] Telefónica UK is a wholly owned subsidiary of Telefónica SA, and belongs to the Telefónica Group, which mainly offers fixed and mobile telephony services in a number of EU Member States as well as in a number of countries outside Europe, in particular in Latin America.

[8] Vodafone Group is the holding company of a group of companies that is involved in the operation of mobile telecommunications network and the provision of related telecommunication services. It is active through its subsidiaries elsewhere in the European Union and in the world through its partner network. Vodafone UK Limited ("Vodafone UK") is the wholly owned subsidiary of Vodafone Group active in particular in the mobile telephony retail market in the UK.

[9] Everything Everywhere is a joint venture created by the merger of T-Mobile UK and Orange UK. It is owned by France Télécom and Deutsche Telekom, which are involved in fixed and mobile telephony services in a number of EU Member States and worldwide.

[10] NFC is a technology standard which enables secure short-range communication between any handset with the relevant chipset in it and another similarly enabled handset (typically a reader), when it is placed within a short distance (typically 3–5 mm).

Finally, the JV Co offers associated data analytics services to its customers, both service providers and advertisers, in respect to the data collected from both its services and the advertising activities. In addition, the customers of the JV Co, both service providers and advertisers, are still free to negotiate with the Parent Companies individually.

The JV Co was created in the new and fast growing sector of mobile commerce which, as said, covers m-payments, mobile advertising and mobile data analytics. In this regard, the European Commission assessed that the notified merger would affect a number of product markets which are nascent and evolving or even not existing in the UK at the time of the filing.

The Definition of the Relevant Markets

In the present case the European Commission investigates seven different relevant product and geographic markets.

Namely the relevant product and geographic markets involved are the markets for:

- the wholesale supply of mobile wallet platforms, which is at least national (correspondent to the UK in the present case) and possibly wider than national in scope;
- the market for secure storage (the market which comprises the provision of secure storage on SIM cards, on embedded SEs, on SEs on devices attached to the mobile handset and cloud-based solutions), which is at least national in scope (UK);
- the downstream market for retail distribution of mobile wallet services to customers, which is at least national in scope (UK) (indeed, the JV Co is not directly active in the retail sector, since it offers a wholesale supply of mobile wallet platforms which enables the Parent Companies themselves as well as other mobile operators or users to offer an individualized mobile wallet for retail on the basis of the mobile wallet platform provided by the JV Co);
- the market for advertising services, national in scope (UK);

- the market for retail and wholesale bulk SMS services (services which enable businesses to send a high volume of text messages to their customers), which is national (UK) or possibly wider;
- the market for data analytics services (which precise geographic market definition has been left open by the European Commission, since the operation would not constitute a hurdle for the existence of effective competition under any alternative geographic market definition); and
- the market for retail mobile telephony services, national in scope (UK).

For the purposes of this chapter it is interesting to further explore the definition of the market for secure storage because it will be seen that it is one of the key relevant product markets in order to assess competition issues in relation to mobile network operators (MNOs).

Indeed, a mobile wallet requires secure storage of information, in particular payment credentials: such storage can be provided by a variety of means such as storage in the cloud and storage on a SE which can be located in various places in or on the mobile device. In such market for secure storage, the issuers of the SE (which, for SIM-based SEs, are the MNOs) control the access to the SE and, therefore, represent the supply side of the market; the demand side is instead represented by retail and wholesale suppliers of wallet solutions. In the present case, control over SIM-based SEs is exercised by their issuers, namely the mobile operators which include the Parent Companies.

Antitrust Regulatory Concerns on Non-Horizontal Assessment

Firstly, there could be a vertical relationship between the market for retail mobile telephony services and the market for the wholesale supply of mobile wallet platform services. In particular, the Parent Companies could exercise a market power in the former market in order to foreclose competition in the market for the wholesale supply of mobile wallet platform services both in terms of inputs by leading to higher prices for service providers (for instance, the foreclosure of essential inputs for the provision of mobile wallets to the end customers such as the SE or

the placement of apps on a mobile handset) and in terms of customer foreclosure.

As to the concern of inputs foreclosure, the European Commission has limited its investigation to assess whether the JV Co has the technical ability to substantially foreclose competing mobile wallet providers through SE means.

Indeed, the European Commission tried to evaluate whether any competitive pressure was exercised on the Parent Companies by means of secure storage other than the SIM-based ones. From the information provided to the European Commission by the Parent Companies and by other competitors, it emerged that—on the one hand—solutions which do not use a SE—like cloud solutions—as well as additional hardware attached to the mobile device are not perfect substitutes for SIM-based SEs, since they are, respectively, less secure and more expensive; however, the European Commission left open whether a market for secure storage comprises also such cloud and hardware solutions, since the merger would not impede effective competition under any alternative product market definition. Hence, an input foreclosure in the market for secure storage is to be excluded in the present case.

Furthermore, SEs embedded in a mobile handset have shown to be close substitutes for a SIM-based SE, having the same security requirements and being perceived as equally secure; moreover, a SIM-based SE and an embedded SE can co-exist on the same mobile handset, thus increasing their degree of substitutability.

Hence, on this aspect the European Commission did not find any incompatibility with competition because there is not a risk of customer foreclosure in the present case providing that if new technologies based on software, cloud-based SEs, NFC stickers or alternative solutions are to come to the market, as could reasonably be expected considering technological evolution, they would provide significant additional competition and subsequently competitive constrains to the JV Co. Additionally, a risk of customer foreclosure could be excluded in the present case, since there are a number of other vertically integrated market players with direct access to end customers (Google or Apple) that do not rely on the access on the market for the wholesale supply of mobile wallet platforms.

As to conglomerate effects no competition concerns arise from the creation of the JV Co. This is because the presence of mobile wallets on mobile devices will not be a determinant factor for consumers when selecting a mobile handset with an MNO. Indeed, although Three UK has pointed out in the present case that the availability of a mobile wallet on a mobile handset is a "must-have" factor for consumers, this possible opinion does not prevent Three UK from offering its own mobile wallet to customers by virtue of the creation of joint ventures with financial institutions or other MNOs as the Parent Companies did in the present case.

Antitrust Regulatory Concerns on Horizontal Assessment

The European Commission examines whether the operation raises horizontal merger effects in consideration of the market for the wholesale supply of mobile wallet platform services, the market for secure storage, and the market for data analytics services.

According to the European Commission's view the markets for mobile wallet platform services and secure storage are not affected by the potential merged entity because they are new markets where many other potential entrants can have access as explained above (such as banks, online and over-the-top players like Google and PayPal). Furthermore, apart from SIM-based SE, access to mobile phones can be also available through embedded SEs, and additional hardware (stickers, tags, etc.). This means that as it has been seen in the assessment for conglomerate and vertical merger effects above, the Parent Companies would not be able to foreclose entrants in the downstream market for retail mobile wallets.

As to the market for data analytics services the European Commission assesses that the operation is not likely to impede effective competition on this market. Indeed, many other strong providers of advertising services are able to offer comparable solutions to the JV Co. In addition, none of the Parent Companies is individually active in the provision of data analytics services in respect of online and offline advertising.

The European Commission's Decision

The European Commission conclude that the joint venture is not likely to impede effective competition, or has the technical or commercial ability as well as the incentive to substantially foreclose entry, or hinder expansion by competitors in relation to the wholesale or retail mobile wallet platform services, advertising services or data analytics.

Indeed, strong players can enter those markets or can emerge in the near future ensuring an adequate competitive pressure. In particular, the European Commission outlines how mobile commerce is an emergent industry where technological developments are always in constant evolution. Hence, alternative solutions for the market of SEs are in progress in the m-payment ecosystem as well as the structure of different mobile wallet platforms. This is important for other players of the m-payment ecosystem (namely, different competitors from MNOs such as Google or Apple) because technological development is likely to provide them with a direct access to end customers.

Conclusions

Mobile commerce is a natural successor to electronic commerce, and it has been forecasted that m-payment is the future alternative to cash and represents a suitable technology for new consumers' necessities.[11] Hence, the importance of a competition law analysis on this topic is vital in order to further develop the diffusion of mobile commerce.

Specifically, thanks to the descriptive analysis, the main issues of competition law within the market for m-payment services can be addressed.

The main actors in m-payment transactions are MNOs, banks and payment systems (Visa, MasterCard, etc.). These operators manage respectively mobile devices, bank accounts and payment platforms. Hence, competition issues in relation to those actors depend on their

[11] Yoris Au, Robert Kauffman, "The economics of mobile payments: understanding stakeholder issues for an emerging financial technology application", *Electronic Commerce Research and Applications* 7 (2008): 142.

degree of cooperation and on the business model that has been adopted. Basically, six different business models have been identified by virtue of economic conventions, but among them[12] the most relevant from a merger efficiency point of view is the full integration business model.[13] In this model banks, MNOs and payment systems collaborate together towards the creation of a joint venture.

However, the joint ventures that have been examined in this chapter constitute only the implementation of a partial integration business model because payment platforms were not involved at all in both cases and banks were involved only in the first merger (Case No. COMP/M. 6956). Hence, the implementation of a full integration business model has not yet been implemented in Europe. This is because the main players of the full integration business model (MNOs, banks and payment systems) are subject to different regulation frameworks that are not yet coordinated and linked by virtue of the enactment of common operating standards.

In relation to merger control aspects, the examined decisions have clearly pointed out that the European Commission will always assess three main merger effects in relation to the creation of joint ventures in the m-payment ecosystem. Firstly, a possible horizontal merger effect concerning the hindering of competition among other players of the relevant product market (such as the market for digital advertising services, the market for the retail distribution of digital wallet, the market for secure storage, etc.). Secondly, a vertical merger effect both related to input and customer foreclosure of competing digital wallet services, and finally a conglomerate merger effect in terms of assessing the existence of tying arrangements or other forms of exclusionary practices.[14]

[12] There are different business models. In the mobile centric model the customers may make a payment to merchants by virtue of his or her mobile phone and this is then charged to the mobile phone bills of the customer. In the same way, in the bank centric model the bank does not collaborate with MNOs and rather the bank starts an m-payment service of its own. The most efficient forms of business from an economic point of view are those that relate to integration between banks and MNOs.

[13] Marc Bourreau, Marianne Verdier, "Cooperation for Innovation in Payment Systems: The case of Mobile Payments", Working Paper in Economics and Social Sciences ESS-10-02, 1–24 (2010): 16.

[14] Indeed, in relation to tying arrangement it should be outlined a distinction between technical tying and contractual tying. According to the former a tying product or service is designed to work

Specifically, in the m-payment ecosystem when either a full integration business model or a partial integration business model is set up in the form of a joint venture there is a potential risk of conglomerate effects[15] due to the complementary relationship that could exist between the issuance of payment cards and the provision of digital wallet services.

On this point, the European Commission (Case No. COMP/M. 6956) has introduced different parameters in order to evaluate the anticompetitive effects of a joint venture in the m-payment industry, and therefore to assess if a possible conglomerate effect is likely to occur. Firstly, the European Commission has to examine whether the joint venture that has been set up by the parent companies has the ability to foreclose competing digital wallets by virtue of restricting the use of payment cards in its digital wallet only to its own cards; secondly, it should be evaluated whether there are sufficient alternative issuers of payment cards and digital wallets, and finally whether there is the possibility of using the payment cards issued by the joint venture in competing digital wallets.

On the other hand, a joint venture can contribute to the creation of market power in relation to MNOs because they are in control of the SE placed inside the SIM (OECD Roundtable on Competition and Payment Systems, 2012). This can lead to the establishment of a vertical or horizontal merger effect (Case No. COMP/M. 6314). As a result, competition might be diminished and innovation in m-payment technologies might be prejudiced.[16] In fact, a player like an MNO that is in control of the SE and is part of a well-established network could abuse its market power by denying access to the established network to new potential entrants; consequently new entrants have to establish their own rival network. As a result, competition might be undermined and at the same time innovation might be prevented.

---

only with the tied product and not with the alternatives offered by competitors; while contractual tying refers to the impossibility of the consumer to purchase other alternative products or services offered by competitors in addition to the tied product or service purchased.

[15] Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings, OJ C 265, 18 October 2008, p. 6, paragraphs 93–94.

[16] Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of the concentrations between undertakings, OJ C 31, 5 February 2004, paragraphs 8 and 38.

Furthermore, the lack of an implemented full integration business model in the m-payment ecosystem in Europe has shown the need for a universal set of standards that could be capable of guaranteeing the interoperability of different implementations.[17] In this regard, the European Banking Authority (EBA) has been recently empowered by the new Regulation on Multilateral Interchange Fees (MIFs) adopted by the Council and the European Parliament[18] and by the new Payment Services Directive (PSD2) that had been adopted by the Council on 2 June 2015 and revised by the European Parliament on 8 October 2015 (the final text to be adopted in the near future by the Council) in order to draft technical standards to promote interoperability in the mobile network payment system solutions, but only with reference to payment service providers. Therefore, the enactment of new standards concerning MNOs is essential in order to harmonize different legislations inside the European Union and to guarantee full network interoperability. If these objectives are achieved, then the likelihood of the establishment of market power positions in relation to the merged entities is avoided. Indeed, nowadays for instance no standards exist to enable consumers to pay, redeem coupons and claim loyalty points at the same time with their mobile handsets.[19] This circumstance would attract in the future the attention of competition regulators that should oversee the process of adoption of standards in order to ensure the participation of every stakeholder operating in the m-payment industry.

In the end, the European legal framework of competition law in relation to m-payments is still in its infancy and must challenge the rapid pace of technological improvements.

[17] Jun Liu, Robert Kauffman, Dan Ma, "Competition, cooperation, and regulation: understanding the evolution of the mobile payments technology ecosystem", *Electronic Commerce Research and Applications* 14 (2015): 382; Andriew S. Lim, "Inter-consortia battles in mobile payments standardisation", *Electronic Commerce Research and Applications* 7, no.2 (2008): 202.

[18] Regulation (EU) No. 751 of 29 April 2015.

[19] Case No. COMP/M. 6314, paragraph 379.

References

Au, Y., & Kauffman, R. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Applications, 7*, 141–164.

Bourreau, M., & Verdier, M. (2010) Cooperation for innovation in payment systems: The case of mobile payments. *Working Paper in Economics and Social Sciences ESS-10-02*, 1–24.

Lim, A. S. (2008). Inter-consortia battles in mobile payments standardisation. *Electronic Commerce Research and Applications, 7*(2), 202–213.

Liu, J., Kauffman, R., & Ma, D. (2015). Competition, cooperation, and regulation: Understanding the evolution of the mobile payments technology ecosystem. *Electronic Commerce Research and Applications, 14*(5), 372–391.

Part IV

Conclusions

12

Mobile Payments and Bitcoin: Concluding Reflections on the Digital Upheaval in Payments

Benjamin Geva

Abstract Mobile payments and bitcoins represent a leap forward in payments. Acknowledging that they are different, yet recognizing a common "digital" denominator, this concluding chapter outlines their salient features in the broad context of the historical evolution of payment mechanisms operated in the framework of a classical model. Thereunder, a payment order issued to a paymaster initiates the transmission of monetary value from a payer-debtor to a payee-creditor. The chapter points out that the mobile payment introduces complexities and variations reflecting its digital nature. At the same time, fundamentally, its operation is premised on that of the classical model. Conversely, not only that Bitcoin introduced new money-equivalent, it is further premised on a decentralized network within which monetary value moves without the involvement of a paymaster.

B. Geva (✉)
Professor of Law, Osgoode Hall Law School, York University, Toronto, Ontario, Canada

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8_12

Introduction: Payment Mechanisms

Mobile payments and bitcoins represent a leap forward in payments. Acknowledging that they work differently, and yet recognizing a common "digital" denominator connecting them, it may be useful to map their features as part of the evolution of non-cash payments or payment mechanisms. To that end I heavily relied on my earlier work,[1] endeavouring to harness it into a picture that will highlight what has stayed the same, what evolved, and what broke new grounds.

"Payment" is broadly defined to mean "any act offered and accepted in performance of a money obligation."[2] In its simplest sense, "payment" signifies the performance of an obligation by the delivery by the payer to the payee[3] of monetary objects, which at present consist of banknotes and coins ("cash"). At the same time, a payment mechanism can broadly be described as any method of payment facilitating the transmission of monetary value, particularly in the form of account debits and credits redeemable to monetary objects that enables the payer to avoid the transportation of monetary objects and their physical delivery to the payee. It also makes monetary objects available for withdrawal.

The operation of a payment mechanism in payment of a debt is premised on the discharge of a debt owed by the payer to the payee by virtue of an authorized payment made by the paymaster. Where the paymaster is the payer's debtor, and to the extent of the sum paid, payment to the payee discharges both the payer's debt to the payee and the paymaster's debt to the payer. Alternatively, not having owed to the payer, a paymaster carrying out payment, besides discharging the payer's debt to the payee, becomes entitled to payment from the payer. Regardless, a paymaster's payment to the payee may be either in monetary objects or by means of

---

[1] Particularly, Benjamin Geva, *The payment order of antiquity and the middle ages*: *A legal history* (Oxford and Portland, Oregon: Hart, 2011), in particular at Ch. 1 [4] (1); Benjamin Geva, *The law of electronic funds transfers* (New York: Matthew bender, loose-leaf) at § 1.04[6].

[2] Charles Proctor, Ed., *Goode on payment obligations in commercial and financial transactions*, 2nd ed. (London: Sweet & Maxwell, 2009), p. 11.

[3] There is no such thing as "a man paying himself." See *Faulkner v. Lowe* (1848), 2 Ex. 595 at 597, 154 E.R. 628 at 630, per Pollock C. (in argument). Hence, "[p]ayment, necessarily implies two distinct persons." John S. James, ed., *Stroud's judicial dictionary of words and phrases*, 5th ed. Vol. 4 (London: Sweet & Maxwell, 1977) *s.v.* "payment" at 1337.

a debt owed to the payee by someone designated by the payee to receive payment. In fact, the paymaster itself may be so designated.

A payment mechanism is initiated by the payer's instructions to a third party ("paymaster") to make the payment. Instructions may be written, electronic, and, under some conditions, oral. Until approximately the middle of the twentieth century payment instructions were predominantly on paper.[4] For example, to this day the *cheque* is a written unconditional order to pay, signed by a "drawer", and addressed to his banker ("drawee").[5] It is issued by the drawer to the payee who takes it as its first "holder"; it may usually be transferred from one holder to another by negotiation, that is, by the delivery of the holder with or without his endorsement.[6] In this process, drawer is debtor, payee is creditor, and banker is paymaster. The cheque is paid by the paymaster upon its presentment by the holder, who usually acts through his own banker; in turn, the holder's banker may entrust one or more bankers to act for him in the process. A payee to whom a cheque is issued is not guaranteed payment and is faced with the risk of dishonour for lack of cover or any other reason.[7]

To protect the payee from the risk of dishonour, the *cheque-guarantee card* was developed. This is an undertaking of the drawee banker, as an issuer-guarantor, to honour debtor's personal cheques. In connection with each cheque issued under the guarantee, the drawee-guarantor's liability injures directly to the benefit of the payee. To benefit from the guarantee, the payee must have taken the cheque on the basis of the guarantee card presented to him at the time of the transaction. In the cheque-guarantee transaction, the drawer is debtor, the payee is creditor, and the drawee-guarantor is paymaster. In contrast to the case of the per-

[4] Excluding other tangible media such as clay in Ancient Mesopotamia, the only exception was face-to-face oral instructions.

[5] See definitions e.g. in s. 73 of the *Bills of Exchange Act, 1882* (UK), 45 & 46 Vict., c. 61 (as am.) ["BEA"]; art. 1 of *Convention providing a uniform law for cheques*, 19 March 1931, 143 L.N.T.S. 355, Annex I ["ULC"]; and §3-104(f) of the *Uniform Commercial Code* Article 3 (1990, as am. 2002) ["U.C.C."]. The order to pay must be for a sum certain in money and the instrument ought to be payable on demand.

[6] BEA s. 31; ULC art. 14; U.C.C. §3-201, *ibid.*

[7] By itself, the issue of the cheque does not constitute a transfer of the cover to the payee, even when such a cover is available in the drawer's account. See e.g. BEA, *ibid.*, s. 53(1).

sonal cheque used without the card, the paymaster in a cheque-guarantee payment is directly liable to the payee-creditor. However, in contrast to the letter of credit, the guarantee is a secondary obligation; it neither discharges the debtor nor is autonomous, namely, free of defences, in the hands of the creditor.[8] Furthermore, from a practical perspective, the cheque-guarantee facility does not involve any communication to the paymaster at the time the cheque is issued. As such, it does not afford the paymaster meaningful protection from fraudulent use. Nor does it offer the paymaster any assurance of limited use within guarantee limits. Therefore, the cheque-guarantee card can work only for small amounts.

Improvement in telecommunication enhanced the position of the payee by affording him or her the issuer's assurance of payment. To that end payment cards[9] were developed outside the cheque system. The first to appear was the *credit card*. Unlike the cheque-guarantee card, the credit card facilitates instant communication from the point of payment to paymaster for authorization. This affords an immediate assurance of payment to the payee-creditor by the paymaster who is able to verify both cover (or more precisely, within credit limits) and whether the card has been reported lost or stolen. Communication between the payee-merchant-creditor and the paymaster was originally over the telephone; now it is electronic; it is from a terminal which "reads" and passes on relevant information from the magnetic stripe on the card when it is swiped by the payee-merchant-creditor at the terminal. Authentication by the cardholder-debtor has typically been by manual signature on a piece of paper which is, however, not a cheque. Thus, without being able to receive online instant authentication from the cardholder-debtor, the paymaster-card issuer is likely to debit a credit line rather than an asset account of the debtor. The latter incurs interest and is to pay the paymaster as of after receiving a periodical statement from paymaster. At the same time, the creditor's banker is typically prepared to instantly

[8] For the secondary obligation of the guarantor, and his release upon breach of the contract, see K. McGuinness, *The law of guarantees*, 2nd ed. (Toronto, Carswell, 1996) at 30–31, 565–66. Contrast with the autonomy of the letter of credit; see Agasha Mugasha, *The law of letters of credit and bank guarantees* (Sydney: The Federation Press, 2003), 136.

[9] See Benjamin Geva, "Consumer liability in unauthorized electronic funds transfers", Canadian Business Law Journal 38 (2003): 207, 212–23.

credit the payee-merchant-creditor's account, albeit provisionally, pending dishonour or return ("chargeback") only on the basis of unauthorized use of the card. In the process, the sales slip signed by the cardholder-buyer-payer-debtor is not even processed; rather, it is kept by the payee-merchant-creditor in case the cardholder claims that the card was used without his authority.

"Electronic banking" started with the electronic interbank processing of paper instructions such as a cheque or even a credit card draft. At least so far as retail payments are concerned, in terms of sound banking practice, authenticated electronic instruction facilitated debit card payments. Thus, the authentication of payment instructions by means of a secret code, such as a PIN, enables the paymaster to promptly, upon authorization, debit the buyer-cardholder-debtor's asset account. This is how, in a process under which the use of payer has been dispensed with, the credit card evolved to a *debit card*, using the same magnetic stripe technology.[10]

The *stored-value card* was developed to eliminate the need to communicate the payment instructions from the point of payment to paymaster for authorization. Unlike credit and debit cards, which are access products facilitating access to value "stored" in an account held with and operated by the paymaster-banker, value in the stored-value card is stored and processed on the card itself. This value has come to be known as "electronic money" or "e-money". Authorization and transfer of value are thus performed on and from the card. This requires an enhanced and sophisticated technology; that of an integrated circuit (IC) card containing a microprocessor chip ("electronic purse"), so as to turn the card into a "smart card".

The legal distinction between credit and debit card continues to turn on the access of the former to a credit line and of the latter to an asset account.[11] However, there is nothing to preclude a card of which use is

[10] See also Benjamin Geva, "The E.F.T. debit card", *Canadian Business Law Journal* 15 (1989): 406.

[11] In the USA, under federal law, the *Consumer Credit Cost Disclosure Act*, 15 U.S.C. §1631 (1968) ["CCCDA"], and Section 226.12 of *Regulation Z Truth in Lending*, 12 C.F.R. §226 (as am.) implementing it, govern a card accessing a credit plan, namely a credit card (defined in Reg. Z §226.2(a)(15)). For a debit card initiating an electronic fund transfer, see *Electronic Funds Transfer Act*, 15 U.S.C. §1693 (1978) ["EFTA"] and *Regulation E* 12 C.F.R. §205 (1981), (as am.) implementing it (particularly its Section 205.3(b)).

premised on PIN authentication, and even on smart card technology, from being linked to a credit line, so as to be a credit card. In fact, with the view of enhancing security and reducing the production of fake cards, there is a growing tendency today towards the use of smart card technology for all payment cards, regardless of whether a given card is an access or stored-value card, and irrespective of whether as an access card it is used in connection with a credit line or an asset account. Still, the preceding analysis demonstrates the evolution of the payment card, providing the creditor with the right to claim from the paymaster, into various uses, in tandem with the advancement of technology.

Finally, payments for small amounts may be made by utilizing NFC, that is, near field communication. Such a payment is carried out by waving next to a RFID (radio-frequency identification)-enabled reader installed on a point of sale (POS) terminal, a card in which a silicon chip and an antenna are imbedded.

From a business perspective, the stored-value card has not fared well. At the same time it allowed an evolution in different directions. First, smart card technology facilitated a next generation of credit cards, called Europay, Mastercard, and Visa, where card payment is secured by a safer PIN authentication. Second, the issuer of the stored-value card is not required to be a bank or any other regulated financial institution. The appearance of a non-bank issuer has become more prominent. Third, to a large extent, the stored-card itself has been replaced by the *prepaid card*, such as a gift, remittance or payroll card which is an access device, albeit not to the cardholder's account, but rather to a master account set up by the card provider (e.g. money transmitter, employer), allowing access for each card to the limits of the "prepayment".[12]

It is at this point of the development of payment methods that digital payments made their first appearance. Their features, nature and suitability for examination in the framework of the aforesaid evolutionary model will now be assessed.

[12] See e.g. Benjamin Geva, "Recent international developments in the law of negotiable instruments and payment and settlement systems", *Texas International Law Journal* 42 (2007): 685, 699–705.

Mobile Payments[13]

Any payment in which a mobile device is used for the purpose of its initiation, activation, and/or confirmation is a mobile payment.[14] Typical mobile devices are the mobile phone, the smartphone, and the tablet.

A mobile payment service may be made available to a bankless segment of the population. As such, it is widely used in developing countries. As well, a mobile payment service can be made available as a category of a broader mobile banking service, facilitating direct access to the subscriber's bank services and information via mobile devices. Either way, the framework for a mobile payment is the traditional architecture of the payment system as described above. Stated otherwise, when the dust settles, it becomes obvious that while introducing variations and some complexities, the mobile payment is initiated by means of a payment order issued to a paymaster who carries it out by paying the payee. In digesting the variations and complexities reflecting the digital nature of this method of payment as set out below, the reader should not lose sight of the fact that the basic payment mechanism model nevertheless underlies the mobile payment.

A mobile payment is carried out pursuant to a data transfer, and is therefore characterized as a digital payment. In making such payment, the mobile device could be used to access a bank account, credit line, or a stored-value or prepaid product. Alternatively, albeit in practice, only for small payments, in what came to be known as a "walled-garden" model,

---

[13] Besides numerous internet and media sources (of which to be particularly mentioned is the monthly *Digital Transactions Magazine*), this section draws on voluminous literature which includes articles published in special issue 27.2 of the Banking and Finance Law Review 226–343 (January 2012); MV Bossuyt and LV Hove, *Mobile payments models and their implications for NextGen MSPs*, 9:5 Journal of Policy, Regulation, and Strategy (August 2007); Rhys Bollen, *Recent developments in mobile banking and payments*, JIBLR (2009): 454; and *Canadian NFC Mobile Payments Reference Model*, CBA 14 May 2012. *See also* SJ Hughes (ed), *RFIDs, Near-Field communications, and mobile payments: A guide for lawyers* (Chicago: ABA, 2013) which has less focus on the payment mechanism itself. For feedback, comments, and information I am grateful to my colleagues at Torys LLP, Peter Aziz and Steven Slavens. All errors are mine.

[14] For a narrower view limiting mobile payments only to those "initiated and transmitted by access devices that are connected to the mobile communication network" as opposed to "payments, such as credit transfers or direct debits, that are only initiated and authorised via the internet using mobile [devices]" see CPSS, *Innovations in retail payments*, Report of the Working Group on Innovations in Retail Payments (Basel: BIS, May 2012): 13.

the device could be used by its holder to buy a product or service directly from the mobile network operator (MNO) and have its price added to the periodic mobile bill. An MNO may also act as a distributor or in some rare cases, an issuer of a stored-value or prepaid product.

Mobile payments present new dimensions to the landscape of non-cash payments. Most notably, they involve communication carriers acting in the payment arena—not as back-office third-party service providers on behalf of banks, but rather, as drivers (or at least co-drivers), sitting in the front seat, in a direct contractual relationship with users. As such, they increasingly seek to provide payment services of their own. Mobile payments also involve an array of non-bank intermediaries, such as merchant aggregators and concentrators. Mobile payment may also facilitate *peer-to-peer* payments made from one stored-value product to another.

An add-on dimension is the ability to receive and use information at the time of making payment. From an issuer's perspective, this may facilitate "upsales". It also allows the issuer to obtain in real time and analyse information as to shopping habits of the customer. This enhances the issuer's ability both to efficiently market to the customer as well as to sell data in which other businesses may be interested. From the customer's perspective, this may facilitate a rational use of resources, such as different accounts or loyalty points, in making payments.

A digital or mobile wallet (m-wallet) is an application that has the ability to carry multiple means of payment. In some way the mobile device can be viewed as a card owned by the end user on which the end user may have diverse applications installed. Placed in the wallet, methods of payment become "connected" and further give access to other facilities and services accessible from the device.[15] In fact, for a wallet to have a successful market penetration it must deliver coupons and offers and, in the long run, even carry important documents routinely carried by individuals such as driving licenses and car insurance certificates. This will mark the obsolescence of the leather wallet—containing all payment cards and documents routinely carried by individuals.

[15] Rogers Communications' David Robinson was quoted to make the following blunt statement: "If you put a bunch of cards into a dead cow, they really don't know each other. But if you put those cards on a phone, that gives you access to a camera, a user ID, a way to know where consumers are, and what they want." *Payment Source*, Emerging Payments Vol.1 No. 1, 26 September 2013.

The wallet provider may be a bank, MNO, as well as a distinct entity acting independently from banks and MNOs. Where the m-wallet is designed so that only the payment applications from the wallet provider may be used to make payment, the wallet is said to be *proprietary*. Conversely, an m-wallet may be designed to accommodate a group of credential issuers in which case it is a *collective* wallet. Only credentials from group members may be bound in a collective wallet. An m-wallet facilitating multiple credential issuers, possibly in collaboration with MNOs and/or wallet providers is an open or *collaborative* wallet.

In communicating credentials from the mobile device to the POS terminal, data security is enhanced by *tokenization*. This is a process by which a sensitive data field is replaced with a surrogate value called a token. De-tokenization is the reverse process of redeeming a token for its associated original value.[16]

To further enhance security, the account and transaction information may reside in a secure element (SE) on the mobile device. The SE may be removable or embedded in the hardware of the mobile device as part of the baseband processor.[17] Alternatively, information accessible through an application from the device may nevertheless be securely stored in the "cloud" outside the device. The removable element can be UICC-SIM based. UICC stands for Universal Integrated Circuit Card. It is a smart card used in mobile terminals networks to ensure the integrity and security of personal data. A smart card is also called a chip card, or integrated circuit card (ICC). It is a pocket-sized card with embedded integrated circuits. An integrated circuit (also referred to as an IC, a chip, or a microchip) is a set of electronic circuits[18] on one small plate ("chip") of

[16] Tokenization is to be distinguished from encryption. The latter is an obfuscation approach that uses a cipher algorithm to mathematically transform sensitive data's original value to a surrogate value. The surrogate can be transformed back to the original value via the use of a "key", which can be thought of as the means to undo the mathematical lock. So while encryption clearly can be used to obfuscate a value, a mathematical link back to its true form still exists. Tokenization is unique in that it completely removes the original data from the systems in which the tokens reside. See e.g. http://perspecsys.com/resources/cloud-tokenization-primer/?pi_ad_id=43615510328&gclid=CND36r38zckCFZAAaQodlX8DOA.

[17] A baseband processor is a device (a chip or part of a chip) in a network interface that manages all the radio functions (that is, all functions that require an antenna). It is separate from the application processor (AP) which is the main processor.

[18] An electronic circuit is composed of individual electronic components, such as resistors, transistors, capacitors, inductors and diodes, connected by conductive wires or traces through which

semiconductor material,[19] normally silicon. SIM is an acronym for "subscriber identity (or identification) module". This is a detachable smart card consisting of an integrated circuit that securely stores on the mobile device the *international mobile subscriber identity* and the related key used to identify and authenticate subscribers on mobile telephone devices.

The SE is either an embedded secure area or secure area in the UICC. It is the place in which encrypted information is stored. It consists of a Secure Domain (SD) and possibly one or more Supplemental Secure Domains (SSDs). Each credential issuer must have its own separate SD or SSD within the SE. Multiple payment applications as well as multiple payment credentials may reside in a single SD or SSD, but only as long as they are from the same credential issuer. An entity that manages access to the SE that stores the end user's sensitive payment credentials on the mobile device and in effect controls the SD or SSD is called a Secure Domain Manager (SDM).

Alternatively, the removable element is an SD card-based SE, which uses the SD card format to provide the security features required by the applications. In NFC products discussed further below, the entity that loads the payment credentials of the end user into the m-wallet application on the end user's device at the request of the credential issuer is called a Trusted Service Manager (TSM).[20] This is a neutral third party entrusted with the transfer of data. It specializes in data-formatting requirements and encryption keys for security loading. By building a bridge between the MNO and payment service providers, the TSM provides interconnectivity that expands the reach of wallets and prevents end users from being locked into a specific wallet application and an MNO.[21]

The credential issuer instructs the TSM to transmit payment credentials to the end user's mobile device. To do this, the TSM liaises with the MNO. Once credentials are on the mobile device, the end user is validated and may use the mobile for making payments.

---

electric current can flow.

[19] A semiconductor is a material which has electrical conductivity to a degree between that of a metal (such as copper) and that of an insulator (such as glass).

[20] The TSM had been mostly involved in NFC payments discussed further below.

[21] It also provides "life cycle management services" such as card deletion from stolen or lost devices as well as where they are not wanted anymore.

As indicated, the alternative to the SE for the safe storage of the account information and payment application is the "cloud". Unlike the SE which is on the device, the "cloud," is effectively in a secure server situated outside the mobile device. It is, however, accessible through an app on the mobile device.

Inasmuch as the distinguishing feature of mobile payments is the involvement of the MNO, it is not surprising that communication technology of stored data plays an important role in figuring out mobile payment fundamentals. Thus, at present, principal methods of digital communication over mobile devices are as follows:

- SMS: Short Message (text) Service—particularly through WIG (Wireless Internet Gateway). This is a menu-driven SIM card application that opens up a channel to the wireless internet on the SIM card so as to facilitate mobile banking by means of a secure SMS. Under this application, a banking menu is downloaded onto the SIM card and encrypted. SMS can also be used to make a payment which is billed by the mobile network carrier as an item on the subscriber's mobile phone bill. This method has become widespread in developing countries.
- NFC: near field communication, premised on a short-range high frequency wireless communication technology, which enables the contactless exchange of data between devices. It is a two-way radio wave protocol that also lets consumers receive and redeem rewards.
- WAP: wireless application protocol for web-based payments. This digital method of communication facilitates the browsing of the web by allowing the mobile device to retrieve information from the internet via a server connected to the cloud on the mobile network. The cloud-linked payment method *may* first require authorization, possibly but not exclusively, via NFC, before enabling the use of the mobile device to gain access to a bank account via the internet. Online payment systems utilize this technology.

  NFC can be used only for "proximity payments" between devices which are located next to each other. SMS and WAP can be used for payments between distant parties (and not only between parties in

proximity). Authentication may be required particularly for relatively high-value amounts. An SMS as well as a NFC payment may be authenticated by entering an alphanumeric password or code.

NFC is a key enabling technology for m-wallets. Relying on the SE in the device, it allows end users to download all their *payment credentials* to the wallet and just tap the device at a POS terminal to transfer via short-range wireless technology funds, coupon, and loyalty information to make a purchase. All elements of the payment application and payment credentials must reside in an SE within the UICC or in an embedded SE area on the mobile device. The NFC wallet requires the installation of a physical NFC chip onto a smart phone. This is a *hardware-based solution* replicating the underpinning of existing systems.

In a cloud wallet, payment and personal information is stored in a secure server, euphemistically described as "cloud". The storage platform or the hosting service in the cloud is called "Dropbox". The information stored in the cloud is accessed through an app on a mobile device or computer. Hence, it is said that in a cloud wallet the "card is in the file". The cloud wallet is a software-driven solution requiring less investment by merchants to accept them at the physical POS. Its secure operation is premised on a tamper resistant module (TRSM) embedded in the merchant POS device (rather than relying on the SE on a phone as in NFC). A TRSM is a device that incorporates physical protections to prevent compromise of critical security parameters (CSP) therein contained. Nothing is stored on the phone—not even the password. A unique access code is generated for the end user. It is device-specific and is generated by entering a complex master password. Once generated, the code is to be kept by the end user separately from the device and yet available for use with it. The password that generated the code need not be memorized. As long as the code was not lost the password is also not to be retained to handy. The password is, however, required for the regeneration of a new code in case the old one is lost.

Host card emulation (HCE) is a hybrid NFC-cloud mobile payment. Initiating a hybrid NFC-cloud mobile payment is a similar process to an NFC-only payment. However, the payment credentials are

not stored locally on the mobile phone. Instead, a virtual account number (or proxy) is used in communication from the mobile phone to a merchant's POS system, which is then used to identify the customer's real payment credentials which are encrypted and stored remotely on servers (the cloud). Neither the merchant nor the mobile phone's operating system has the real payment card information. This method of payment allows banks and other wallet providers to bypass the MNO, who controls the SIM card (and the fees set up by it), on which the NFC-only payment has depended.

Bitcoin[22]

Bitcoin is a peer-to-peer payment network and digital currency based on an open source protocol, which makes use of a public transaction log. It was introduced in 2009 by pseudonymous developer Satoshi Nakamoto. A bitcoin does not represent a claim to a physical object or to a physical currency—it aims to be in itself a currency. It substitutes a physical object as well as a credit to a bank account with a *computer file*—containing a list of all past transactions with a unit as of its creation. Bitcoin is a fiduciary currency. As it has no intrinsic value it is not a commodity-based currency. Moreover, there is no paymaster carrying out the debtor's instructions; rather it is the debtor who, by utilizing the procedure outlined below, causes bitcoins to move from one wallet to another.

In making a payment, the payer requests an update to a public transaction log, the blockchain. This master list of all transactions shows who owns what bitcoins—currently and in the past. It is maintained by a decentralized network that verifies and timestamps payments using a proof-of-work system. Bitcoin is a cryptocurrency because it uses public-key cryptography to control the creation and transfer of the computer file which purports to be "money". Users send payments by broadcasting digitally-signed messages to the network. Participants known as miners

[22] Conventionally "Bitcoin" capitalized refers to the technology and network whereas "bitcoins" lowercase refers to the currency itself. The gist of the ensuing discussion is based on Benjamin Geva, Preliminary Report to MOCOMILA Meeting in Washington DC April 2014.

verify and timestamp transactions into a shared public database called the blockchain, for which they are rewarded with transaction fees and newly "minted" bitcoins.

Upon payment with bitcoins, the Bitcoin protocol ascertains the payer's ownership in the file—and validates its transfer to the payee. The protocol also regulates issue of bitcoins; it defeats counterfeiting and double spending; and ensures the safe transfer of the computer file. It does all that without relying on a single authority.

The blockchain is a public ledger of every bitcoin transaction that provides a certain level of anonymity. Thus, it identifies transactions by Bitcoin address and not by individual names. However, tracking the flow of bitcoins through transactions can give clues as to who the owner is. As well, while Bitcoin uses cryptography, it does not do so to protect the identities of its users. In addition, Bitcoin intermediaries such as exchanges are required by law in many jurisdictions to collect personal customer data.

Development process relies heavily on community "rough" consensus. The gatekeeping function by "core developers" includes control over the infrastructure and the conduct of discussions on patches to the protocol. Since the Bitcoin Foundation of 2012, a US self-regulatory body called the Data Asset Transfer Authority (DATA), was formed. Its mission: standardizing, protecting and promoting the Bitcoin project.

The acceptance of bitcoins in payment of goods and services raises significant issues as to the protection of the public. Also, as a privately issued currency, Bitcoin raises a challenge to conventions on the meaning of money that have crystalized for thousands of years. The acceptance of its ideas by libertarian thinkers and politicians certainly raises its profile. Specific legal issues include:

- Legal nature of "computer file"? Is it a claim? Against whom?
- Who is liable for the [nominal?] value?
- Is it in fact "money", currency, commodity or intangible? Even if it is not "legal tender" or "official currency", is it "money" as a matter of statutory interpretation [e.g. BEA, SGA], particularly when it is agreed to be a means of payment? Is it "money" by its mere acceptance as a means of payment?

- Is it subject to securities regulation?
- Does its use impact monetary policy?
- How is it governed by anti-money laundering?
- How is it as a subject for taxation?

So far no uniformity has been achieved in the treatment of all such issues.

In the long run, I am not persuaded that Bitcoin as a money-substitute will seriously challenge fiat money issued by central banks. Certainly, I see no problem with its circulation in payment of debt as well as with its serving as a medium of account. At the same time, I am more sceptical as to Bitcoin storing stable value.[23] Perhaps I should point out that historically the issue of both coins and banknotes originated under the hands of private enterprise, except that the state was quite quick to take over.[24] However, history needs not necessarily repeat itself and perhaps I am too hasty in counting on it.

This however does dispense with the need to regulate Bitcoin for the protection of the public. Treatment ought to be at least harmonized if not uniform. Hence the importance of an ongoing discussion on the subject. Furthermore, one aspect of Bitcoin is destined to stay and revolutionize payment transactions.

Thus, Bitcoin is both a money-substitute and a method of payment over a blockchain. The blockchain is a specific technology for a virtual ledger, known also as a public distributed ledger, which is a record of transactions shared among ledger users. It is used to verify the permanence of transactions as well as to prevent double spending and malicious attacks. The virtual ledger may be used to link each pair of banks for a payment between them without the use of an intermediary even in the absence of a correspondent relationship between them.

More in general, at present, banks exchange customers' payment instructions and pay each other resulting amounts owed in the

[23] For the features of money as a unit of account, medium of exchange and storage of stable value, see e.g. N Dodd, *The sociology of money*: *Economic*, *reason* & *contemporary society* (New York: Continuum, 1994) at xv.

[24] For coins such was the case in Lydia around the seventh century BCE. For banknotes such was the case in England in the course of the eighteenth century CE. See Geva, *The payment order*, above note 1 at 84–85 and 476–489 respectively.

exchange. The interbank exchange is termed a "clearing" and the ensuing payment is termed a "settlement". In a clearing, payment instructions may be processed either manually or in an automated system, and either in bulk or individually. Payment instructions may be settled either bilaterally or multilaterally, as well as either on a deferred net settlement basis (DNS) or in real time such as in an RTGS (real-time gross settlement) system. Typically, for each official currency, at least the large banks settle on the books of the central bank of the country of the currency. A small bank may settle on the books of a large bank acting as its correspondent. For its part, a non-bank payment service provider requires the services of a bank for both incoming and outgoing customers' payments.

In bypassing any need for both intermediation and multibank clearing activities, the virtual ledger is bound to pose a challenge to payment laws that have been premised on payment carried out over accounts of banks.

Conclusion

Both mobile payments and Bitcoin heralded a new era of digital payments. Herein lies the rationale for treating the legal challenge they pose in one volume. Both developments open new avenues and yet give rise to new challenges. However, in the final analysis, mobile payments reflect an evolution that fits into the conceptual framework of the payment mechanism as it has evolved over the years. They introduce new players in new roles and yet have not changed the basic architecture of the payment system.

This is certainly not so with respect to Bitcoin. Not only does Bitcoin provide for a novel type of money. Rather, it has also paved the way for a new architecture for the payment system. This is a true conceptual revolution which may require more than the adaptation of existing laws.

Being the arena for activity for both novel methods of digital payments, the Single Digital Market has thus been correctly identified as a common target for a harmonized if not uniform regulation in the European Union. While highlighting and certainly not obfuscating the

fundamental distinction between mobile payments and cryptocurrencies such as Bitcoin, pursuing this task ought to be encouraged.

References

Bollen, R. (2009). Recent developments in mobile banking and payments. *JIBLR, 454*, 154–469.

Bossuyt, M. V., & Hove, L. V. (2007). Mobile payments models and their implications for NextGen MSPs. *Journal of Policy*, *Regulation*, *and Strategy, 9*(5), 31–43.

Canadian NFC Mobile Payments Reference Model. (2012). CBA 14 May 2012.

CPSS. (2012, May). *Innovations in retail payments*. Report of the Working Group on Innovations in Retail Payments. Basel: BIS.

Dodd, N. (1994). *The sociology of money: Economic, reason & contemporary society*. New York: Continuum.

Geva, B. (1989). The E.F.T. debit card. *Canadian Business Law Journal, 15*, 406–440.

Geva, B. (1992). *The law of electronic funds transfers* (1st ed.). New York: Matthew Bender, Loose-Leaf.

Geva, B. (2007). Recent international developments in the law of negotiable instruments and payment and settlement systems. *Texas International Law Journal, 42*, 685–726.

Geva, B. (2011). *The payment order of antiquity and the middle ages: A legal history*. Oxford and Portland, Oregon: Hart.

Hughes, S. J. (Ed.) (2013). *RFIDs. Near-field communications, and mobile payments: A guide for lawyers*. Chicago: ABA.

James, J. S. (Ed.). (1977). *Stroud's judicial dictionary of words and phrases* (Vol. 4, 5th ed.). London: Sweet & Maxwell.

McGuinness, K. (1996). *The law of guarantees* (2nd ed.). Toronto: Carswell.

Mugasha, A. (2003). *The law of letters of credit and bank guarantees*. Sydney: The Federation Press.

Proctor, C. (Ed.) (2009). *Goode on payment obligations in commercial and financial transactions* (2nd ed.). London: Sweet & Maxwell.

The Regulatory Challenges Ahead

This book has examined mobile payments and virtual currencies, above all the Bitcoin, as the most widespread virtual currency scheme within the European Union framework, paying specific attention to regulatory experience beyond EU borders. Lastly, investigation from a historical perspective has revealed the global vocation of payments and the law of payments. Indeed, through time, the law of payments has tried to provide easy-to-handle rules for the debtor and creditor within the monetary obligation and any intermediaries involved so that traders and consumers can not only buy and sell, but also transfer funds far away, all the while guaranteeing them legal certainty regarding the end payment and the allocation of responsibility. The question is, has the EU already reached this goal?

The volume has underlined how the European Union has been steadily working since the late 80s to produce a single framework for payment services while building up a single currency area. The European Union has moved from soft laws on the use of credit cards and distance payments, including European Court of Justice case law on the freedom of capital and payments, and now issues directives on credit transfers and e-money institutions. Recently, the EU policymaker has set out a comprehensive legal and regulatory framework for payments based upon

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8

the concept of the "payment service". The flexible concept of "payment service" has allowed the European Union to move on with both the integration process for payment and financial services and to launch a plan for a single digital area.

However, the interdisciplinary and cross-sectoral approach of this book has allowed us to address some controversial issues that need to be dealt with:

- Firstly, the approach to law-making. When the lawmaker—either the European or a foreign lawmaker—is required to face the regulatory challenges posed by new access devices or innovative means of payment, namely the Bitcoin and mobile payments, it tends to have the same attitude: legal systems adapt to unfamiliar circumstances and try to regulate the new, using the old. This approach might pose the risk of resorting excessively to analogy, extending the application of rules and regulations without providing the necessary supervision or authorization.
- Secondly, the dialectical relationship between general and sector-based regulation. The comprehensive framework for payment services, as laid down in the Payment Services Directive (PSD) and its update (PSD2), may make it possible to tackle the main issues linked to innovative payment services, but a strong sector-based regulation seems to be needed to deal with transaction security, personal data protection and money laundering control.
- Thirdly, market-driven regulation. The European policymaker has strongly driven a levelling of the market and has encouraged innovation. However, any effort made in this direction should be accompanied by awareness of the fact that the evolution of payment systems based mainly or exclusively on a profit maximization approach would ill accord with the assumption that the proper operation of payment system is a public interest function.
- Finally, it has correctly been stressed that mobile payments and the Bitcoin are only the last result of the process of market globalization. This means that the European Union's efforts to lay down a harmonized framework must be appreciated, but both of them are naturally

cross-border instruments, so consistent standards should be encouraged across the jurisdictions.

In the end, the European Union has made many steps forward but much is still to be done.

Bibliography

Aghion, P., Nicholas, B., Richard, B., Rachel, G., & Peter, H. (2005). Competition and innovation: An inverted-U relationship. *Quarterly Journal of Economics*, 120(2), 701–728.

Aghion, P., Ufuk, A., & Peter, H. (2015). The Schumpeterian growth paradigm. *Annual Review of Economics, 7*, 557–575.

Alberts, J., & Fry, B. (2015). Is Bitcoin a security? *Boston University Journal of Science & Technology Law, 21*, 1–21.

Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014a). The economics of digital currencies. *Bank of England Quarterly Bulletin, 54*(3), 276–286.

Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014b). Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin, 54*(3), 262–275.

Ametrano, Ferdinando M. "Hayek Money: the Cryptocurrency Price Stability Solution." (August 19, 2014). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270)

Arangüena, G. (2014). Bitcoin: una sfida per policymakers e regolatori. *Diritto mercato tecnologia. Quaderno Anno IV*(1), 19–43.

Article 29 Working Party. (2013). *Opinion 02/2013 on apps on smart devices*. WP 202, 27 February. Brussels.

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8

Au, Y., & Kauffman, R. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Application, 7*(2), 141–164.

Badev, A., & Chen, M. (2014, October). Bitcoin: Technical background and data analysis. *Federal Reserve Board Finance and Economics discussion series*, 2014–104.

Bal, A. (2013, July). Stateless virtual money in the tax system. *European Taxation*.

Baldwin, R., Scott, C., & Christopher, H. (Eds.). (1998). *A reader on regulation.* Oxford: Oxford University Press.

Banca d'Italia. (2015, January 30). Avvertenza sull'utilizzo delle cosiddette valute virtuali. Rome.

Bank of International Settlement. (2012, May). *Innovation in retail payments*. Basle: Committee on Payment and Settlement Systems.

BEUC, The European Consumer Organisation. (2012). *Towards an integrated European market for card, internet and mobile payments: European Commission Consultation on the Green Paper.*

Blind, K. (2010). The use of the regulatory framework to innovation policy. In R. Smits, P. Shapira, & S. Kuhlmann. (Eds.), *The theory and practice of innovation policy – An international research handbook.* Cheltenham: Edward Elgar.

Board of Governors of the Federal Reserve System. (2015, March). Consumers and mobile financial services 2015. Washington.

Bollen, R. (2013). The legal status of online currencies: Are Bitcoins the future? *Journal of Banking and Finance Law and Practice, 24*, 272–293. http://sites.thomsonreuters.com.au/journals/files/2013/12/WAU-Jnl-Bank-Law-Fin-Vol-24-No-4-Dec-13-Contents.pdf.

Bolt, W. (2012, December). Retail payment systems: Competition, innovation, and implications. DNB Working Paper n. 362. 1–32.

Borchgrevink, J. (2014, January 9). Warning: GHash.IO is nearing 51% – Leave the pool. *Crypto Coins News*. https://www.cryptocoinsnews.com/warning-ghash-io-nearing-51-leave-pool/

Bossuyt, M. V., & Hove, L. V. (2007). Mobile payments models and their implications for NextGen MSPs. *Journal of Policy, Regulation, and Strategy, 9*(5).

Bourreau, M., & Marianne, V. (2010). Cooperation for innovation in payment systems: The case of mobile payments. Working Paper in Economics and Social Sciences ESS-10-02. 1–24.

Bradford, T. et al. (2009). Nonbanks and risk in retail payments: EU and U.S. In M. Eric Jonhson (Ed.), *Managing information risk and the economics of security* (pp. 17–53). Berlin: Springer.

Brandolini, A., & Emanuela, C. (Forthcoming). L'ambigua relazione tra concorrenza e crescita. In A. Gigliobianco, & G. Toniolo. (Eds.), *Concorrenza, mercati e crescita in Italia: il lungo periodo.* Venezia: Marsilio.

Brito, J., Castillo, A., & Shadab, H. B. (2014). Bitcoin financial regulation: Securities, derivatives, prediction markets, and gambling. *Columbia Science and Technology Law Review, 16*, 146–221.

Camenisch, J. L., Piveteau, J.-M., & Stadler, M. A. (1994). Security in electronic payment systems. Institute for Theoretical Computer Science, ETH Zurich. In: *Proceedings of the ESO RISKS* 94.

Canadian NFC Mobile Payments Reference Model. (2012, May 14). CBA.

Chatain, P.-L. (2008). Integrity in mobile phone financial services, measures for mitigating risks from money laundering and terrorist financing. *The World Bank Working Paper* No. 146. Washington, DC.

Ciani, D., & Masi, P. (2014). Integration of EU payment systems: A 'tolerable straight line'? *Ianus Special Issue,* 7–23.

Clarkson, E. C., Patel, S. N., Pierce, J. S., & Abowd, G. D. (2006). Exploring continuous pressure input for mobile phones.

Colesanti, J. S. (2014). Trotting out the white horse: How the S.E.C. can handle Bitcoin's threat to American investors. *Syracuse Law Review, 65*, 1–52.

Committee on Payment and Market Infrastructures (CPMI). (2015, November). *Report on digital currencies.* Basle: CPMI.

Committee on Payments and Market Infrastrcuture (CPMI). (2015, September). The World Bank Group. Consultative Report. Payment Aspects of Financial Inclusion. 1–77. http://www.bis.org/cpmi/publ/d133.pdf

Committee on Payments and Market Infrastructures. (2014, September). *Non-banks in retail payments*, Bank for International Settlements, Basle, 1–47.

Committee on Payments and Market Infrastructures (CPMI) and World Bank Group. (2015). *Consultative report on Payment aspects of financial inclusion*. Bank for International Settlements and World Bank Group.

Committee on Payments Settlement Systems (CPSS). (2012, May). Innovations in retail payments, 1–96. http://www.bis.org/cpmi/publ/d102.htm

Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions, "A Digital Single Market for Europe", Brussels 6.5.2015, COM (2015) 192 final, 1–20.

Consultative Group to Assist the Poor (CGAP). (2012). *Financial consumer protection regulation in Europe/Central Asia*.

Continie, D., et al. (2012). *M-payments in the United States: Mapping the road ahead*. Boston, MA: Federal Reserve Bank of Boston, Federal Reserve Bank of Atlanta.

Cuéllar, M.-F. (2003). The Tenuous relationship between the fight against money laundering and the disruption of criminal finance. *Journal of Criminal Law and Criminology,* 93, 311–465. http://ssrn.com/abstract=354740. Accessed 15 Aug 2015.

Dapp, T.-F. (2012). *The future of (mobile) payments: New (online) players competing with banks*. Frankfurt am Main, Germany: Deutsche Bank Research.

Dapp, T. F., Stobbe, A., & Wruuck, P. (2012, December 20). *The future of (mobile) payments: New (online) players competing with banks.* Deutsche Bank Research.

De Azevedo C., & Viola, M. (2013). *Market integration through data protection: An analysis of the insurance and financial industries in the EU.* Dordrecht: Springer.

De Azevedo C., Viola, M., Marin, L., & Sartori, G. (2012). Peer-to-peer privacy violations and ISP liability: Data protection in the user-generated web. *International Data Privacy Law, 2*(2), 50–67.

De Filippi, P. (2014). Bitcoin: A regulatory nightmare to a libertarian dream. *Internet Policy Review, 3*(2), 1–12.

Dennehy, D., & Sammon, D. (2015). Trends in mobile payments research: A literature review. *Journal of Innovation management, 3*(1), 49–61.

Desai, S. (2014). Mobile payment services: Security risks, trends and countermeasures. RSA Conference 2014, Asia Pacific & Japan.

Desjardins, J. (2014, August 13). How secure are Bitcoins?. *Visual Capitalist.* www.visualcapitalist.com/secure-bitcoins/

Di Castri, S. et al. (2011). *Consumer protection diagnostic study*. Kenya, Nairobi: Financial Sector Deepening Kenya.

Dodd, N. (1994). *The sociology of money: Economic, reason & contemporary society*. New York: Continuum.

Doguet, J. J. (2013). The nature of the form: Legal and regulatory issues surrounding the Bitcoin digital currency system. *Louisiana Law Review,* 73(4), 1119–1153.

Doherty, C. (2014). Bitcoin and bankruptcy – Understanding the newest potential commodity. *ABI Journal,* 33(7), 28–33.

Elwell, C. K., Murphy, M. M., & Seitzinger, M. V. (2013). *Bitcoin: Questions, answers and analysis of legal issues*. Washington, DC: Congressional Research Service.

Enria, A. (2015, September 28). The single rulebook in banking: Is it 'single' enough? In *Lectio Magistralis*. Padova: University of Padova.

EU Commission. (2007, December 12). Commission encourages swift and coherent implementation at national level, *press release IP/07/1914.* http://europa.eu/rapid/press-release_IP-07-1914_en.htm?locale=en

Eurofinas. (2015). Eurofinas observations on the Commission's proposal for a directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. COM(2013) 45 final http://www.eurofinas.org/uploads/documents/positions/AML/Eurofinas observations - final.pdf. Accessed 15 Oct 2015.

European Banking Authority. (2014, July 4). *EBA opinion on virtual currencies.*

European Banking Authority – EBA. (2013, December). *Warning to consumers on virtual currencies.* 13.

European Banking Authority (EBA). (2014, July). *Opinion on 'virtual currencies'.* https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014 08+Opinion+on+Virtual+Currencies.pdf

European Banking Authority (EBA). (2015). EBA opinion on virtual currencies. https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf. Accessed 13 Oct 2015.

European Banking Federation (EBF). (2012, April 10). *EBF position on the European Commission's Green Paper 'Towards an integrated European market for card, internet and mobile payments'.*

European Central Bank. (2009, December). Retail payments – Integration and innovation. Frankfurt.

European Central Bank. (2011, October). The future of retail payments: Opportunities and challenges. Frankfurt.

European Central Bank. (2012, October). Virtual currency schemes. Frankfurt. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

European Central Bank. (2013). Recommendations for the security of mobile payments, draft document for public consultations. https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf?7f9004f1cbbec932447c1db2c84fc4e9

European Central Bank. (2013, November). Recommendations for the security of mobile payments. Frankfurt.

European Central Bank. (2014, June). Retail payments at a crossroads: Economies, strategies and future policies. Frankfurt.

European Central Bank. (2014, October). Mandate of the European Forum on the security of retail payments.

European Central Bank. (2015). Virtual currency schemes – A further analysis. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf. Accessed 20 Aug 2015.

European Commission. (2012a, November 1). *Green Paper towards an integrated European market for card, internet and mobile payment*s. COM(2011) 941 final, Brussels: EC.

European Commission. (2012b). *Green Paper*: *Towards an integrated European market for card, internet and m-payments.* Brussels: EC.

European Commission. (2012, January 25). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation*), COM(2012) 11 final, Brussels: EC.

European Commission, Directorate-General for Research and Innovation. (2013, October 30). Final Report from the Expert Group on Retail Sector Innovation. http://ec.europa.eu/research/innovation-union/pdf/Report_from_EG_on_Retail_Sector_Innovation_A4_FINAL_2.pdf

European Commission. Proposal for a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing COM(2013) 45 final.

European Commission. *Proposal for a directive of The European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC*, COM/2013/0547 final.

European Data Protection Supervisor (EDPS). (2013, December 5). *Opinion of the European data protection supervisor on a proposal for a directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and Repealing Directive 2007/64/EC, and for a Regulation of the European Parliament and of the Council on interchange fees for Card-Based payment transactions*. Brussels: EDPS.

European Parliament. (2015). *Legislative resolution of 8 October 2015 on the proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC (COM(2013)0547 – C7-0230/2013 – 2013/0264(COD))* (Ordinary legislative procedure: first reading), P8_TA(2015)0346.

European Payment Council. (2012, October). White paper. Mobile payments.

European Payment Council. (2014, April 29). EPC comments on the draft recommendation for the security of mobile payments developed by the European Forum on security of retail payments. *European Payments Council Newsletter.*

European Payment Council. (2014, January). White paper. Mobile wallet payments.

European Payment Council. (2014, December). Overview on mobile payments initiatives. EPC091-14, Version 2.0.

European Payment Council. (2015, August 7). *Summer reading: Results of latest EPC poll reveal that instant payments are most likely trigger the next wave of innovation* (blog).

European Payment Council and GSM Association. (2010, October). *Mobile contactless payments service management roles requirements and specifications*.

Europol. (2015). The Internet Organized Crime Threat Assessment (IOCTA).

Fairfield, J. (2015). Bitproperty. *Southern California Law Review, 88*, 807–874.

Farmer, P. H., Jr. (2014). Speculative tech: The Bitcoin legal quagmire & the need for legal innovation. *Journal of Business & Technology Law, 9*, 85–106.

Financial Action Task Force. (2014, June). Virtual currencies. Key definitions and potential AML/CFT Risks. http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Financial Action Task Force – FATF. (2013, June). *Guidance to a risk-based approach to prepaid cards, mobile payments and internet based payments services*. Paris.

Financial Action Task Force – FATF. (2014, June). *Virtual currencies key definitions and potential AML/CFT risks*. Paris.

Financial Action Task Force (FATF). (2014). Guidance for a risk-based approach. The Banking sector. FATF/OECD.

Financial Action Task Force (FATF). (2015). International standards on combating money laundering and the financing of terrorism & proliferation ("The FATF Recommendations"). http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf. Accessed 15 Aug 2015.

Financial Action Task Force (FATF). (2015). Money laundering using new payment methods. http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf. Accessed 13 Oct 2015.

Financial Action Task Force (FATF). (2015). Guidance for a risk-based approach – Virtual currencies. http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. Accessed 15 Aug 2015.

Financial crimes enforcement network – FinCEN. (2013, March 18). Application of FinCEN's regulations to persons administering exchanging or using virtual currencies. FIN 2013-001.

Financial crimes enforcement network – FinCEN. (2014, October 27). Request for administrative ruling on the application of FinCEN's regulation to a virtual currency payment system.

Geva, B. (2007). Recent international developments in the law of negotiable instruments and payment and settlement systems. *Texas International Law Journal, 42*, 685–726.

Geva, B. (2011). *The payment order of antiquity and the Middle Ages: A legal history*. Oxford and Portland, Oregon: Hart.

Geva, B. (1992). *The law of electronic funds transfers.* New York: Matthew bender, loose-leaf.

Geva, B. (1989). The E.F.T. debit card. *Canadian Business Law Journal, 15*, 406–440.

Gibney, C. et al. (2015, January). *International review: Mobile payments and consumer protection.* Financial Consumer Agency of Canada.

Gilkes, P. (2011). Liberty dollars may be subject to seizure. Coin World Publications.

Gloria, G. F. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Dordrecht: Springer.

Goldman Sachs. (2014, March 11). All about Bitcoin. *Top of Mind*, Issue 21.

Goodhart, C., Llewellyn, D., & Hartmann, P. (1997). Reflections on financial regulation. *Financial Stability Review,* London: Bank of England, *3*, 51–60.

Grinberg, R. (2011). Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal, 4*, 159–208.

Gup, B. E. (2014). What is money? From commodities to virtual currencies/ Bitcoin. http://ssrn.com/abstract=2409172. Accessed 15 Aug 2015.

Gwen, D., & Kronenberg, D. E. (2014). Bitcoins in bankruptcy: Trouble ahead for investors and Bankruptcy professionals? *Pratt's Journal of Bankruptcy Law,* 10(2), 112–121.

H.M. Treasury. (2015, March 18). *Digital currencies: Call for information*.

Hancher, L., & Moran, M. (1998). Organising regulatory space. In R. Baldwin, C. Scott, & C. Hood (Ed.), *A reader on regulation.* Oxford: Oxford University Press.

Herzberg, A. (2003). Payments and banking with mobile personal devices. *Communications of the ACM*, *46*(5), 53–58. Chicago.

Hoofnagle, C. J., Urban, J. M., &and Li, S. (2012). Mobile payments: Consumer benefits & new privacy concerns. *BCLT Research Paper*.

Howden, E. (2015). The crypto-currency conundrum: Regulating an uncertain future. *Emory International Law Review, 29,* 742–798.

Hughes, S. J., & Middlebrook, S. T. (2014). Regulating cryptocurrencies in the United States: Current issues and future directions. *William Mitchell Law Review, 40*, 813–848.

Hughes, S. J. (Ed.). (2013). *RFIDs. Near-field communications, and mobile payments—A guide for lawyers.* Chicago: ABA.

Hughes, S. J., & Middlebrook, S. T. (2013). Virtual uncertainty: Developments in the law of electronic payments and financial services. *Indiana University Legal Studies Research Paper Series*.

Information Systems Audit and Control Association (ISACA). (2011, November) Mobile payments: Risk, security and assurance issues. *An ISACA Emerging Technology White Paper*. http://www.isaca.org/groups/professional-english/pci-compliance/groupdocuments/mobilepaymentswp.pdf

Internal Market Directorate (2007), *Payment System Directive. What it means for consumers*, Available at http://ec.europa.eu/internal_market/payments/docs/framework/psd_consumers/psd_en.pdf

International Finance Corporation (IFC). (2011). Mobile money study: Summary report.

Jack, W., & Suri, T. (2011, January). Mobile money: The economics of M-Pesa. *NBER Working paper*, No. 16721.

James, J. S. (Ed.). (1977). *Stroud's judicial dictionary of words and phrases* (5th ed., Vol. 4). London: Sweet & Maxwell.

Jeans, E. D. (2015). Funny money or the fall of Fiat: Bitcoin and the forward-facing virtual currency regulation. *Journal on Telecommunications and High Technology Law, 13*, 100–127.

Kaplanov, N. M. (2012a). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *Loyola Consumer Law Review, 25*, 111–171. http://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1920&context=lclr.

Kaplanov, N. M. (2012b). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *Temple University Legal Studies Research Paper* No. 25, 1–46. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203

Kasiyanto, S. (2015). Regulating peer-to-peer network currency: Lessons from Napster and payment systems. *Journal of Law, Technology and Public Policy, 1*(2), 40–73.

Kasiyanto, S. (Forthcoming). Moving forward, bringing Bitcoin into the mainstream.

Kemp, R. (2013). Mobile payments: Current and emerging regulatory and contracting issues. *Computer Law & Security Review, 29*, 175–79.

Kiaonarong, T. (2014). Oversight issues in mobile payments. IMF Working Papers No. 123, 1–35.

Kien-Meng Ly, M. (2014). Coining Bitcoin's "Legal-Bits": Examining the regulatory framework for Bitcoin and virtual currencies. *Harvard Journal of Law & Technology,* 27(2), 587–605.

Kim, C., Wang, T., Shin, N., & Kim, K.-S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications, 9*(1), 84–95.

Kosta, E. (2013). *Consent in European data protection law*. The Hague: Martinus Nijhoff.

Krohn-Grimberghe, A., & Sorge, C. (2013, August). Practical aspects of the Bitcoin system. *The Computing Research Repository (CoRR)*.

Krueger, M. (2001, August). The future of M-payments: Business options and policy issues. Electronic Payment Systems Observatory, Institute for Prospective Technological Studies, Joint Rsearch Center, European Commission, Report EUR 19934 EN, 1–24. To download from epso.jrc.es/Docs/Backgrnd-2.pdf.

Larson, J. (2015). Bitcoin: Same song, second verse, a little bit louder and little bit worse. *Michigan Tax Law, 41*, 34–37.

Law Library of Congress (2014, January). *Regulation of Bitcoin in selected jurisdictions*. http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

Lederman, L. (2007). 'Stranger than Fiction': Taxing virtual worlds. *NYU Law Review, 82*, 1621–1672.

Lee Kuo Chuen, D. (Ed.). (2015). *Handbook of digital currencies*. Amsterdam: Academic Press.

Leith, P. (2012). Europe's Information Society project and digital inclusion: Universal service obligations or social solidarity? *International Journal of Law and Information Technology, 20*(2), 102–123.

Lim, A. S. (2008). Inter-consortia battles in mobile payments standardisation. *Electronic Commerce Research and Applications,* 7(2), 202–213.

Linck, K., Pousttchi, K., & Wiedemann, D. G. (2006). Security issues in mobile payment from the customer viewpoint. MPRA Paper No. 2923. 1–10.

Liu, J., Kauffman, R., & Ma, D. (2015). Competition, cooperation, and regulation: Understanding the evolution of the mobile payments technology ecosystem. *Electronic Commerce Research and Applications, 14*(5), 372–391.

Lo, S., & Wang, C. (2014, September). Bitcoin as money? *Current perspectives*, Federal Reserve Bank of Boston, n. 14–4.

Luther, W. J. (2015). Regulating Bitcoin: On what grounds? Available at SSRN: http://ssrn.com/abstract=2631307. Accessed 20 Aug 2015.

Maioli, C., & Perugini, M. L. (2014). *Bitcoin tra Moneta Virtuale e Commodity Finanziaria.* University of Bologna – Research Center of History of Law, Philosophy and Sociology of Law, and Computer Science and Law, 1–40.

Malaguti, M. C. (2009). The payment services directive. Pitfalls between the Acquis Communitarie and National Implementation. *ECRI Research Report*, *9*, 1–32.

Mallat, N. (2007). Exploring consumer adoption of mobile payments – A qualitative study. *Journal of Strategic Information Systems, 16*, 413–432.

Mann, F. (1971). *The legal aspect of money*. Oxford: At the Clarendon Press.

McGuinness, K. (1996). *The law of guarantees* (2nd ed.). Toronto: Carswell.

Meredith, M. W., & Tu, K. V. (2015). Rethinking virtual currency regulation in the Bitcoin age. *Washington Law Review, 90*, 272–347.

Mitsilegas, V., & Gilmore, B. (2007). The EU legislative framework against money laundering and terrorist finance: A critical analysis in the light of evolving global standards. *International & Comparative Law Quarterly,* 56(1), 119–140.

Mittal, S. (2013). Is Bitcoin money? Bitcoin and alternate theories of money. Independent Writing Project.

Mobile Payments Industry Workgroup (MPIWG). (2012). *The US regulatory landscape for mobile payments*. Federal Reserve Bank of Atlanta and Federal Reserve Bank of Boston. Available at https://www.bostonfed.org/bankinfo/payment-strategies/publications/2012/us-regulatory-landscape-for-mobile-payments.pdf

Moody's. (2013, February). Moody's analytics: The impact of electronic payments on economic growth 1–18. at online: https://usa.visa.com/dam/VCOM/download/corporate/media/moodys-economy-white-paper-feb-2013.pdf.

Mugasha, A. (2003). *The law of letters of credit and Bank guarantees*. Sydney: The Federation Press.

Nakamoto, S. (2008a). *Bitcoin: A peer-to-peer electronic cash system.* Available online: http://nakamotoinstitute.org/bitcoin/#selection-7.4-13.16

Nakamoto, S. (2008b). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Accessed 20 August 2015.

Naqvi, M., & Southgate, J. (2013). Banknotes, local currencies and central bank objectives. *Bank of England Quarterly Bulletin, 53*(4), 317–325.

OECD. (2012). *Recommendation of the council on regulatory policy and governance*. Paris: OECD.

Okuttah, M. (2012). *M-Pesa drives Safaricom as profit declines to Sh12.8bn*, *Business Daily*, Available at http://www.businessdailyafrica.com/Corporate+News/MPesa+drives+Safaricom+as+profit+declines+/-/539550/1403606/-/35hl1b/-/index.html

Ondrus, J., & Pigneur, Y. (2009). Near field communication: An assessment for future payment systems. *Information Systems and E-Business Management, 7*(3), 347–361.

Organisation for Economic Co-operation and Development (OECD). (2014). *The governance of regulators*. Paris: OECD.

Pacy, E. P. (2014). Tales from the cryptocurrency: On Bitcoin, square pegs, and round holes. *New England Law Review, 49*, 122–144.

Pak Nian, L., & Lee Kuo Chuen, D. (2015). Introduction to Bitcoin. In Lee Kuo Chuen, D. (Ed.), *Handbook of digital currencies* (pp. 6–30). Amsterdam: Academic Press.

Pegueros, V. (2012). Security of mobile banking and payments. *SANS Institute InfoSec Reading Room*.

Pelkmans, J., & Andrea, R. (2014, November). Does EU regulation hinder or stimulate innovation? Centre for European Policy Studies (CEPS)*, Special Report*, Bruxelles: CEPS no.96.

Perugini, M. L., & Maioli, C. *Bitcoin:* tra moneta virtuale e *commodity* finanziaria. Available at http://ssrn.com/abstract=2526207

Plassaras, N. A. (2013). Regulating digital currencies: Bringing Bitcoin within the reach of the IMF. *Chicago Journal of International Law, 14*, 377–407.

Pousttchi, K., & Wiedemann, D. G. (2007). What influences consumers' intention to use mobile payments. *Mobile Communications Working Group, University of Augsburg*. http://www.marshall.usc.edu/assets/025/7534.pdf

Proctor, C. (Ed.). (2009). *Goode on payment obligations in commercial and financial transactions* (2d ed.). London: Sweet & Maxwell.

Rahn, R. W. (2010). A constant unit of account. *Cato Journal, 30*(3), 521–533.

Ramasastry, A. (2014). Bitcoin: If You can't ban it, should you regulate it? The merits of legalization. *Justia.com*

Reid F., & Harrigan, M. (2013). An analysis of anonymity in the Bitcoin system. In Y. Altshuler et al. (Eds.), *Security and privacy in social networks* (pp. 197–223). Dordrecht: Springer.

Report from the Commission to the European Parliament, the Council and the Economic and Social Committee, Brussels. COM (2003) 702 final, 1–25.

Rode, L. (2006). Database security breach notification statutes: Does placing the responsibility on the true victim increase data security. *Houston Law Review, 43*, 1597.

Rosenfeld, M. (2012, December 13). Analysis of hash-rate-based double-spending. Latest version: Available at https://bitcoil.co.il/Doublespend.pdf

Rösl, G. (2006). Regional currencies in Germany: Local competition for Euro? *Deutsche Bundesbank, Discussion paper series 1*: Economic Studies n. 43.

Schmiedel, H., Kostova, G. L., & Ruttenberg, W. (2012). The social and private costs of retail payment instruments: A European perspective. *ECB Occasional paper* No. 137.

Schoenmakers, B. (1997). Basic security of the e-cash payment system. *Computer security and industrial Cryptography: State of the art and evolution, LNCS series*.

Schroeder, R. (2013, June 19–23). *The financing of complementary currencies: Risks and chances on the path toward sustainable regional economics.* The 2nd international conference on complementary currency systems, The Hague.

Selgin, G. (2013a). *Synthetic commodity money*. The Cato Institute University of Georgia. Athens.

Selgin, G. (2013b, April 10). Synthetic commodity money. Available at SSRN: http://ssrn.com/abstract=2000118

Shadab, H. B. (2014). Regulating Bitcoin and block chain derivatives. Written Statement to the Commodity Futures Trading Commission, Global Markets Advisory Committee, Digital Currency Introduction.

Shy, O. (2005). *The economics of network industries*. Cambridge: Cambridge University Press.

Sirer, E. G. (2014, March 1). What did not happen at Mt. Gox.

Sonderegger, D. (2015). A regulatory and economic perplexity: Bitcoin needs just a bit of regulation. *Washington University Journal of Law & Policy, 47*(175), 175–216.

Souppaya, M., & Scarfone, K. (2013). Guidelines for managing the security of mobile devices in the enterprise. *NIST Special Publication*, 800.

Sullivan, R. J. (2014). Controlling security risk and fraud in payment systems. *Federal Reserve Bank of Kansas City, Economic Review, 99*(3), 47–78.

Sultana, R. (2009). *Mobile banking: Overview of regulatory framework in emerging markets*. Bangladesh: Grameenphone Ltd.

Swartz, N. D. (2014). Bursting the Bitcoin bubble: The case to regulate digital currency as a security or commodity. *Tulane Journal Technology & Intellectual Property, 17*, 320–335.

TALOS Vulnerability Report. (2015, September 15). MiniUPNP internet gateway device protocol XML parser buffer overflow. TALOS-2015-0035. http://talosintel.com/reports/TALOS-2015-0035/

The Economist. (2015, October 31). Blockchains: The great chain of being sure about things.

The World Bank. (2012, October 1–20). From remittance to M-payments. http://siteresources.worldbank.org/EXTPAYMENTREMMITTANCE/Resources/WB2012_Mobile_Payments.pdf

Trautman, L. (2014). Virtual currencies Bitcoin & what now after liberty reserve, Silk Road, and Mt. Gox?. *Richmond Journal of Law and Technology,* 20, Available at http://jolt.richmond.edu/v20i4/article13.pdf

Turban, E., & Brahm, J. (2000). Smart card-based electronic card payment systems in the transportation industry. *Journal of Organizational Computing and Electronic Commerce, 10*(4), 281–293.

United States General Accountability Office – GAO. (2014, May). *Virtual currencies*.

Vaishampayan, D. S. (2013). Bitcoins are private money in Germany. *Wall Street Journal, The Tell* (blog)

Valant, J. (2015, June). European Parliamentary Research Service. Consumer protection aspects of Mobile Payments. European Parliament Briefing. http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564354/EPRS_BRI%282015%29564354_EN.pdf. Accessed 12 Oct 2015.

Valcke, P., Vandezande, N., & Van de Velde, N. (2015). The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4. Swift Institute Working Paper No. 2015-001, http://www.swiftinstitute.org/wp-content/uploads/2015/09/SIWP-No-2015-001-AML-Risks-of-the-Third-Party-Payment-Providers_FINAL.pdf. Accessed 13 Oct 2015.

Vandezande, N (2013). Mobile wallets and virtual alternative currencies under the EU legal framework on electronic payments. ICRI Working Papers No. 16, 1–28.

Velde, F. (2013, December). Bitcoin: A primer. *Chicago FED letters*, Federal Reserve Bank of Chicago.

Visa Europe Risk Management. (2014). Secure mobile payment systems, recommendations for building, managing and deploying. Visa Europe.

Visco, I. (2015, May 7). Remarks, *Harnessing financial education to spur entrepreneurship and innovation*. 3rd OECD/GFLEC Global Policy Research Symposium to Advance Financial Literacy. Paris: OECD.

Wallace, B. (2011). The rise and fall of Bitcoin. *Wired Magazine*, San Francisco

Weber, B. (2014). Can Bitcoin compete with money? *Journal of Peer Production, 4*, Available at http://peerproduction.net/issues/issue-4-value-and-currency/invited-comments/can-bitcoincompete-with-money/

White, L. H. (2014). The troubling suppression of competition from alternative monies: The cases of the Liberty Dollar and E-gold. George Mason University, Department of Economics, Working Paper No.6, 1–30.

Wile, R (2014, July 20). One of Bitcoin's strongest backers reveals the two big reasons why it's still not mainstream. Available at http://www.businessinsider.com/fred-wilson-on-bitcoin-2014-7?IR=T

Winklevoss, C. (2014). What may have happened at Mt.Gox. https://winklevosscapital.com/what-may-have-happened-at-mt-gox/

Wolf, R. (2010). The sad history of carbon carousels. *VAT Monitor* No. 6.

Wolf, R. (2014). Bitcoin and the EU VAT. *International VAT Monitor*. September/October. 254–257.

Yermack, D. (2013, December). Is Bitcoin a real currency? An economic appraisal. NBER Working Paper No. 19747.

Yermack, D. (2015). Is Bitcoin a real currency? An economic appraisal. In D. Lee Kuo Chuen (Ed.), *Handbook of digital currencies* (pp. 31–44). Amsterdam: Academic Press.

Ziskina, J. (2015). The other side of the coin: The Fec's move to approve cryptocurrency's use and deny its viability. *Washington Journal of Law Technology and Arts, 10*, 306–327.

Index

G. Gimigliano (ed.), *Bitcoin and Mobile Payments*,
DOI 10.1057/978-1-137-57512-8