Money after Money: disassembling Value/Information Infrastructures

MONEY AFTER MONEY

disassembling value/information infrastructures

Valeria Ferrari

Promotiecommissie

Promotores:	*prof. dr. M.R.F. Senftleben*	Universiteit van Amsterdam
	dr. B. Bodó	Universiteit van Amsterdam
Copromotores:	*dr. J.P. Poort*	Universiteit van Amsterdam
Overige leden:	*prof. dr. M. de Goede*	Universiteit van Amsterdam
	prof. dr. A.M. Pacces	Universiteit van Amsterdam
	prof. dr. E.L.O. Keymolen	Tilburg University Universiteit
	dr. K. Irion	van Amsterdam Goethe
	dr. C. Westermeier	University Frankfurt
	prof. dr. M.A. Campbell Verduyn	Rijksuniversiteit Groningen
	prof. dr. M. Bartl	Universiteit van Amsterdam

Faculteit der Rechtsgeleerdheid

Layout and cover design: Andy Díaz Sánchez

Contact
Institute of Network Cultures
Email: info@networkcultures.org
Web: www.networkcultures.org

Published by the Institute of Network Cultures, Amsterdam, 2023.

institute of
network cultures

This research has received the financial support of the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under grant agreement No 759681.

Valeria Ferrari

MONEY AFTER MONEY: DISASSEMBLING VALUE/INFORMATION INFRASTRUCTURES

Conosco gente che fa i soldi con la coca.
Sembra che compra i soldi con la droga.

Massimo Pericolo

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

API	Application Programming Interface
BIS	Bank for International Settlements
BSA	U.S. Bank Secrecy Act
CBDC	Central Bank Digital Currency
CESR	Committee of European Securities Regulators
CSDs	Central Securities Depositories
DLTs	Distributed Ledger Technologies
EBA	European Banking Authority
ECB	European Central Bank
EFIP	European Forum for Innovation in Payments
EMD2	Electronic Money Directive 2
ERPB	Euro Retail Payments Board
ESMA	European Securities and Markets Authority
FATF	Financial Action Task Force
FinCEN	U.S. Financial Crimes Enforcement Network
FSC	Financial Stability Committee (EU)
ICO	Initial Coin Offering
MiFID II	Markets in Financial Instruments Directive
MiFIR	Markets in Financial Instruments Regulation
MTF	Multilateral Trading Facility
NCAs	National Competent Authorities
OTF	Organised Trading Facility
PSD2	Payment Services Directive 2
REC	Real Economy Currency
RM	Regulated Market
SEPA	Single Euro Payments Area

PREFACE
SURF AND SOUND

In the fall of 2016, during the last year of my law degree, my criminology professor took me on as an intern in his research center "e-Crime", dedicated to investigating the intersections between criminal law, criminology, and ITCs. During my internship, I was assigned to an EU-funded project, named "Surf and Sound", aimed at studying the role of the Internet in processes of human trafficking and illegal "smuggling" of migrants. My tasks, for this project, were pretty straightforward: I had to find and collect evidence of human trafficking and facilitation of illegal migration online. "Online" meant, literally, any "place" I could access with my computer. I found myself navigating platforms like Instagram and Facebook, and exploring obscure websites in the dark web, to find marketplaces offering fake and stolen documents, trips by boat to reach Europe from Libya or Turkey, sexual services, and so on.

A great many questions raced through my mind during that research; a lot of confused "whys?", "hows?" and "whos?". It struck me how countless "illegal" markets of indefinite dimensions existed all over the web, managed through social media accounts on mainstream platforms, on dedicated websites, or reachable through tentative searches with the Tor engine. Nothing dangerous or complicated was necessary to access them; they were just there, so ubiquitous and so unnoticed. I soon started gathering information about Bitcoin, the currency in use in these dark markets. It was accepted in exchange of weapons, human organs, drugs. But it also allowed to acquire censored books, and documents which would allow people to flee countries and seek protection elsewhere. So it was a currency for criminal activity,

but also a currency for escaping censorship, a currency of rebellion and, in a sense, of "freedom".

Bitcoin and other emerging cryptocurrencies were not entirely a new story. Blockchain technology and cryptocurrencies brought together "long existing ideas in a new constellation" (Bodó, Giannopoulou, 2019, p.2): they emerged as the latest product of an ideology which places *decentralization* as a normative design option for technologies meant to be censorship-resistant and immune from centralized, top-down forms of power. Bitcoin was, in other words, reproposing the idea that decentralized systems based on technocratic governance can underpin novel modes of social, political, and economic organization, circumventing states, institutions, and law enforcement. This is an ideology of decentralization that has written the history of the Web, with returning waves of hope and failures.

I understood decentralized systems like Tor and the Bitcoin network as technologies built with the intention of evading law enforcement. I also understood them as tools of political emancipation, and bottom-up forms of organization, as they embed values (e.g., confidentiality, transparency), rules for access, transaction management as well as media of value in their design and architecture.

In somewhat similar but also opposite ways, global technology companies exploit code to insulate themselves from external jurisdictions. Through technological architecture, they enforce restrictions, and conditions of access and use, to solidify networks of dependencies, establishing forms of sovereignty across markets, expanding through various scales and geographies.

These understandings were the start of my interest in the tensions between digital technology and the law as conflicting forms of social ordering. I discovered a rich academic literature on the complex and ever-evolving relationship between legal systems and digital environments. Law can directly regulate and direct the development of digital technologies, with various degrees of specificity and intensity (Dommering, 2006, pp. 6-7). In turn, technological development influences law, demanding legal change and the adaptation of political agendas. Finally, code itself can exert a regulatory capacity, either

when it is exploited by governments to pursue their own goals (so-called regtech), or when it is used by businesses or individuals to operate forms of private regulation, such as in the case of commercial platforms or cryptocurrency ecosystems.

The desire to disentangle the multifaceted relationship between legal and technological power, and to understand the ways in which it evolves and plays out in the development of digital infrastructures, is the main driver of this thesis.

INTERDISCIPLINARITY, SPEED, AND SPECULATION

Different conceptual and interpretative scaffoldings have assisted me in writing the four articles presented here. At times I have wondered whether it has been a methodological mistake to not select fewer of them, and follow a narrower, better-defined methodological path.

Along the way, I have found myself overwhelmed by the number of academic trajectories that I could have taken, the legal questions I could have tried to untangle in an attempt to address the broader dilemmas that motivated my academic journey (e.g., How are intermediary liability regimes applied in the context of decentralized technologies? Which actors in a blockchain network are responsible under the GDPR?). All these trajectories offered valid lenses of analysis, presenting pressing and stimulating legal questions. However, they all at some point turned out to be shorthanded, blind to certain aspects of the problem, and missing other, equally valid versions of the story. When solving a legal compliance issue, questions regarding the policymaking process, the ideas, the values, and the *imaginaries* informing such policymaking emerged. When reflecting on law enforcement-related issues, questions about the shape and affordances of the technical infrastructure became relevant: which norms were embedded within the code, and which were not? Who wrote that code, and under what incentives?

This kind of thinking, expanding in all directions within and beyond various fields of law, breaching boundaries between disciplines, translates into interdisciplinary research design and methods.

Interdisciplinarity presents a scholar (especially a Ph.D. student) with many challenges. The first one is personal and existential: the problem of not belonging to a single academic community. Whether I went to information law, finance or political science academic events, I would feel like a stranger: never speaking my own language, always borrowing terms that I would discard in the next paper, always learning a bit of everything without becoming an expert in anything.

Such lack of belonging is strictly dependent on the second kind of issue that interdisciplinarity entails: a linguistic one. Sitting at the intersection of information law, finance, social science and computer science, my research taps into a highly specific, yet contested terminology. Thinking critically about the relationship between technological, legal, and societal change requires constant efforts of translation: deciphering, contextualizing, and transferring terms that, when brought from one context, or from one subject, to another often change meaning and interpretation.

When studying processes of change that have impacts at technological, legal, and societal levels, interdisciplinarity is only the first, most obvious methodological challenge. Along the way, I realized that my research was facing two other interconnected obstacles: first, the fact that the object of study is in flux, incessantly changing, at a speed that outpaces researchers' capacity to identify and discuss the relevant issues; second, the fact that the technology observed, as well as the regulatory reactions to it, were speculative in nature, projected rather than materialized. I was looking at institutional interventions against techno-social changes that were invoked or feared, potential rather than already concretized. Hence, the efforts of a researcher in this field are inevitably speculative on two levels: because of the speed of change, it needs to predict techno-legal developments of technologies that are already per se of a speculative nature.

Due to the speculative nature of my inquiry, the exact scope of my Ph.D. has been continuously redefined over time. I proceeded by trial and error, testing the waters in different domains of policy, looking for the next relevant intersection of legal and socio-technical developments. This also motivated the choice of a paper-based Ph.D. This research format allows me to deal with emerging socio-legal issues in a timelier manner, to look in various

places before identifying the next relevant thing to focus on, to experiment, to adjust my trajectory along the way, to talk about issues as soon as they come up, and before they become obsolete.

This way of proceeding is reflected in the policymaking process itself: observatories, expert groups, reports, public consultations, and the so-called "wait and see" approach represent the policy of the "if" – of the conditional, of the fears and hopes, of the attempts to steer society toward one of the many possible futures. Law is supposed to evolve, and change, along with society and the technologies that are produced by it. But digital technology presents us with a pace of change that institutional processes are not designed to keep up with. Law struggles to find mechanisms which allow the dynamism and constant redefinition required by rapidly changing technological systems. Examples of such an effort can be found, for example, in the EU's Digital Services Act, which encourages future regulators to "keep up to date" with the legal requirements through amendments enacted by delegated acts, when the material conditions make such amendments necessary. But this sacrifices certainty, predictability, and a sense of stability of the law.

Another way institutions react to the problem of dangerous transformation is by creating themselves infrastructures to anticipate, steer, or prevent exogenous transformative powers.[1] But this approach always requires making normative decisions about what socio-technical imaginaries can be endorsed, legitimized, and materialized through institutional processes. The role of the legal scholar, therefore, becomes that of measuring how policymaking attunes with the rhythms of technological and social change: whether they synchronize or set on different temporalities, projecting and materializing similar or radically different futures.

---

1 This is, for example, the case of the digital euro: an institutional response to big political threats through non-legal but infrastructural change. As a material expression of power, the digital euro is both a ceremonial manifestation of power and an instrumental, possibly despotic form of infrastructural power.

CHAPTER 1: INTRODUCTION

The entire subject sits at the intersection of two fields that are notoriously prone to hype-based obfuscation – computer tech and finance –, and inherits a lot of bad habits from both, with a reputation for making things deliberately more difficult to understand, specifically to create the illusion that only they are smart enough to understand it.

DAN OLSON, *Line Goes Up – The Problem With NFTs*

Fig. 1: Dogecoin to the moon

Digital value transfer infrastructures are complex techno-social systems, the production and control of which is contested by a plurality of actors and powers.

The creation of digitally native "currencies" circulating over distributed, worldwide networks of computers is, at least symbolically, one of the biggest provocations that Internet subcultures have posed to state sovereignty. Created by radical groups of liberal, anti-state technologists, these transaction systems are designed to evade the control of states and the legacy of financial institutions.

At different layers of the Internet stack, technology companies organized as platforms integrate financial transactions within their expanding networks of services, in order to capture and valorize financial data (Mejias, 2019; Sadowski, 2019), strengthening mechanisms of users' enclosure within their digital ecosystems. While witnessing and reacting to these two coexisting technological developments, public institutions, at various scales, propose the construction of digital value transfer infrastructures built as public utilities.

This manuscript is a journey through coexisting, emerging, or speculated-about types of digital value transfer infrastructures. Using digital money and payment networks as a central case study, this thesis is concerned with unpacking the negotiation processes that shape the governance, design, and political purposes of digital infrastructures that are closely linked to public interest and state sovereignty.

In particular, the papers that are assembled in this manuscript identify and inspect three main socio-technical developments occurring in the domain of value transfer technologies: a) the privatization and platformization of digital payment infrastructures; b) the spread of blockchain-based digital value transfer infrastructures; and c) the construction of digital value transfer infrastructures by public institutions.

Concerned with the relationship between law, discourse, and technological development, the thesis explores four transversal issues that reveal differences and peculiarities within the three scenarios mentioned above: i) privacy; ii) the

synergy and mutual influence of legal change and technological development in the construction of digital infrastructures; iii) the role of socio-technical imaginaries in policymaking concerned with digital infrastructures; and iv) the geography and scale of digital infrastructures.

1.1 AN INQUIRY INTO INFRASTRUCTURES' POWER

In the articles that compose this thesis, I deploy the lens of infrastructure power (Easterling, 2014) to shed light on the co-dependence and interactions between social systems of meaning, political processes, technical rules, and material artifacts as they come to govern and organize our lives.

As socio-material artifacts, infrastructures are studied as the concrete manifestation of hidden and explicit power dynamics, of systems of exploitation, and processes of exclusion. Infrastructures shape, enable, and limit social, economic, and administrative practices; they embed affordances, politics of inclusion and exclusion, privileges, and discriminatory practices. They are simultaneously "things", such as railways, pipes, cables, and computer servers, and processes involving human interactions – networks of relationships among institutions, commercial actors, workers, and objects.

Serving as a medium for monetary exchanges, government transfers, and trading, financial infrastructures are particularly crucial to political economies, administrative processes, law enforcement and, ultimately, the exercise of sovereignty. Traditional financial infrastructures are infrastructures for the transfer of value as captured by the official currency of the state. States also like to control value transfer infrastructures with substantial socio-economic roles, such as those for the circulation of cigarettes, gold, gas, and essential raw materials.

The digitization of money and payment has, in recent years, exposed multiple possible directions of development for the future of value transfer infrastructures: possible technological architectures with correspondent configurations of power; and different types of literacies (Larkin, 2013). The current landscape of actual or speculative digital value transfer infrastructure, therefore, poses compelling questions about legitimacy, authority, agency, and legal change in processes of infrastructural and digital transformation.

It is often the collapse of critical infrastructures, and the threat (or promise) of radical change, which puts into the spotlight previously hidden, or backgrounded, socio-technical processes. The 2008 financial crisis, the recent Covid-19 pandemic, and the sanction regimes following the start of the Ukraine war reminded us of the powerful impact that institutions and material artifacts underpinning financial movement can exert on our lives, both as individuals and as political communities. Such awareness is a crucial starting point for much-needed scrutiny into the entangled relationship between money, its digital (im)materiality, the narratives that are attached to it, and the powers that lie beneath it.

The emergence of new types of infrastructures that materialize and circulate value offers an excellent case study that highlights how infrastructures produce and move political agency from public to private actors, from localized places to virtually traced geographies. It illustrates, furthermore, how the evolution of social narratives and imaginaries drive change even in highly technical fields at the intersection of law, politics, and digital technologies.

Deploying digital value transfer infrastructures as a starting case study, the insights offered by this manuscript are meant to inform a broader understanding of the relationship between technological artifacts, law, and discourse in processes of institutional and infrastructural change.

1.2 AREA OF STUDY AND GLOSSARY OF OPERATIONALIZED TERMS

This thesis deals with issues raised by emerging models of digital infrastructures that organize and mediate value circulation. In doing this, it is not concerned with financial or economic matters. Rather, by offering a critical assessment of specific technologies of value transfer, it brings to the fore issues that lie at the core of information law: the production, circulation, and use of information; and the societal practices and power relations they produce and reproduce. And it proposes, to address these issues, a toolset that is typical of information law: privacy, mechanisms of law enforcement, policymaking, and public intervention in the making of digital infrastructures.

Recent changes in the technologies of money raise questions that have little to do with monetary policy. These changes, Prasad (2021) argues, affect, for example, the accessibility of financial services, which become matters of digital literacy and digital access. Having direct and looming impacts on privacy and transaction confidentiality, digital transactions systems will pull banking and other payment intermediaries into discussions about ethical uses of data, and put them under scrutiny around citizens' surveillance (Prasad, 2021, p. 22). Organized as an information infrastructure, central bank digital money would not only work as a stable medium of exchange, but could also serve as a "tool enabling the implementation of various government economic and social policies" (Prasad, 2021, p. 22).

The shifting frameworks of the social functions of money coincide with the shifting materials of money.[2] New and compelling questions raised by the evolution of digital infrastructures for value circulation are not questions of coinage or of price stability (while these aspects might also be affected by the socio-technical developments analyzed in this thesis, it is outside of the thesis' scope to assess that). Rather, they are questions about the networks and data flows that enable and constitute financial transactions. The meaning of "monetary power" is transforming: it is not only about the purchasing power of one currency over another, but also the control over the networks, cables and databases that enable money flows.

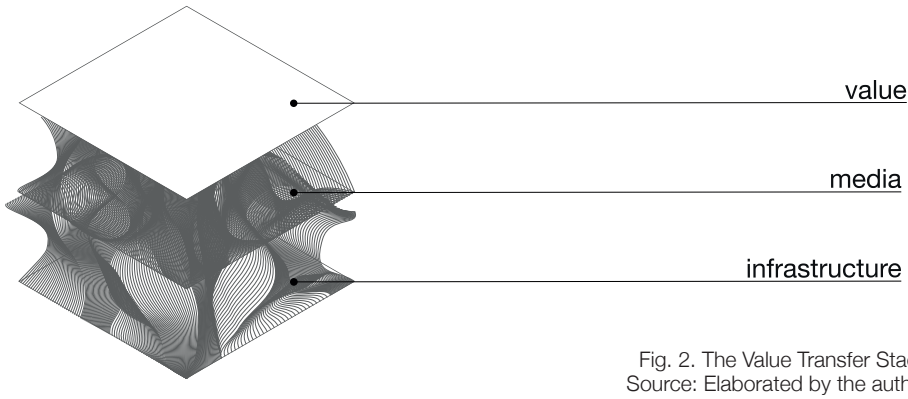

Fig. 2. The Value Transfer Stack.
Source: Elaborated by the author.

2 The distinction between *money proper* and the media that enables its embodiment and circulation is not a recent intuition. See, for example, Giddens, in The consequences of modernity, 1990: "Today, 'money proper' is independent of the means whereby it is represented, taking the form of pure information lodged as figures in a computer printout" (p. 25).

Different digital infrastructures of value circulation emerge, along with value "tokens", which is media (money) embedded in specific technologies. This thesis deals with the technologies, and political and social relations that enable those systems of value to exist and perform their mediation function

In Figure 2, I illustrate the separation between *value*, the *media* that embodies that value – which we sometimes can call *money*, or more simply, *token* –, and the *infrastructure* upon which the latter circulates. The ensemble of the three layers is what I call the *stack of value transfer*.

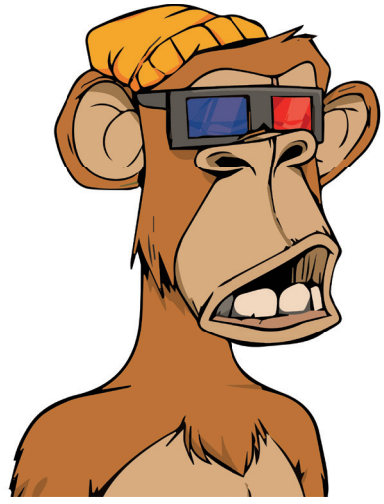

Fig 3: Sample of the Bored Ape Yacht Club, an NFT Monkey collection attacked to the Ethereum blockchain which features algorithmically-generated cartoon profile pictures.

This figure does not aim to signify that the three layers are independent from each other; on the contrary, value is not independent from the media, and the infrastructure in which it is embedded. Moreover, the infrastructure layer encompasses the other two layers, as it is the materialization and institutionalization of the relationships between them. The infrastructure is also constitutive of the media as it determines its conditions of existence and circulation. Leaving aside economic reasonings around value creation, and questions about the specific features of the media, I focus on the infrastructure layer, which I refer to as *digital value transfer infrastructure*. This implies

observing the social construction of value transfer infrastructures, and the social function they fulfill, therefore revealing important preconditions for value creation and its embeddedness in digital media.

Considering value as that surplus on a material (or digital) object that transforms such an object in media (Galloway, 2006), I refrain from going into the question of what forms that surplus – this is a question economists have dealt with, and keep dealing with, without coming to a unequivocal answer. I also do not tackle what projects value onto individual tokens: whether scarcity alone, some intrinsic value, provenance, or aura (Benjamin, 1968), or collective speculation.

The question of whether Bitcoin, and other cryptocurrencies, can be qualified as money – although a very interesting one – is also not specifically addressed in this manuscript. The classification and consequential legal treatment of blockchain-based tokens based on their exact function is dealt with in Chapter 3. I do not delve further into this question here, as I like to think of the general findings of my thesis as applying regardless of whether value transfer infrastructures enable the circulation of money, art, securities, digital rights, or illicit goods. If anything, what is interesting about blockchain is that it has, to a certain extent, abolished the separations between these domains. It has collapsed money, financial assets, and art into one generic media, circulating over the same digital infrastructure; and it has shown that an entry on a ledger can be an alleged copyright claim, a payment entry, and a stake in a company all at the same time.

The identification of tokens' functions became a matter of relevance only *ex-post*; a concern for the regulators who needed to fit them into pre-defined categories. This thesis focuses on the transactional aspects of exchange systems – the architectures of data flows and their policy implications, the networks of relationships and power dynamics that such systems enable – rather than on the static qualities of tokens. In any case, the latter constantly change over time.

As different legal regimes may apply to the same token, different legal regimes may apply to the infrastructure itself. Blockchain-based digital currencies networks can be regulated as financial infrastructures, but also

as telecommunication infrastructures; nodes can be considered as data controllers, as data processors under the GDPR, as well as settlement systems under MiFID.[3]

The relevance and originality of my contribution, I believe, lies exactly in bringing concepts and instruments developed in the field of information law into a domain of study that has traditionally been left outside of the scope of information law scholars. I operate a translation of questions that I view as necessary, as infrastructures of value circulation must be addressed not only as financial infrastructures but as information infrastructures, when the value they circulate is materialized as digital media.

In this guise, my thesis crosses disciplinary boundaries and talks to academics in various domains, hoping to lend useful critical tools born within information law but increasingly relevant in the study of value transfer systems. This cross-disciplinary aspect inevitably implies some limitations. I deploy terms that have different, more specific meanings in different disciplines.[4] This is an issue, I believe, not only of my thesis, but of a domain of study that lies at the intersection of law, finance, technology, political science, and anthropology. I try to deal with this shortcoming by offering a small "glossary" of relevant terms below. The aim of this glossary is not to provide exhaustive definitions, but rather to help the reader understand what notions inform my gaze, and my critical evaluations.

---

3 See Chapter X. Paper by me and Alex on blockchain and GDPR. See also: https://www.paradigm.xyz/2022/09/base-layer-neutrality.

4 Note, for example, that a legal definition of money does not exist. The issue of what electronic or digital money is, is not solved by the Electronic Money Directive, which simply defines electronic money as: "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer" (EMD Article 2(2)).

Money

Academics have never come to an agreement on the exact definition of money. Orthodox economics textbooks generally describe money as 1) a unit of account which serves as 2) a medium of exchange, and/or as 3) a store of value. This definition, however, is not used by anthropologists, sociologists, or historians, who focus instead on money's social construction. According to Ingham, for example, commodity theories of money conceal the nature of money as a social artifact made of infrastructures and people (Ingham, 2004). Dodd argues that fundamental to the legitimation of money is the existence of a "foundational myth", which results from the interplay between technical theories (economics and finance) and meaning (orderly ways of connecting the past and the future) (Dodd, 2016).

Drawing upon these theories, Du Pont suggests thinking about cryptocurrencies' moneyness as a layered assemblage of economic/technical theories and beliefs. The bedrock strata of this assemblage is the "mathematical certainty of cryptographic algorithms"; on top of it is the belief in "cyberspace as a place with its own laws, rules, and norms, […] a global market free from the impediments of national boundaries"; the top strata, finally, is composed of ever-changing, variable multiple protocols that organize single digital currencies' circulation (Du Pont, 2019, p.120).

Relevant to my study is the description of money as discursive practice; as social and cultural narrative (Agha, 2017; Coeckelbergh and Reijers, 2016). These accounts underline the linkages between money and the community that recognizes it, not only in terms of authority but also in terms of semiotics.

Another relevant concept that emerges in various theories of money is that of a claim against something. Debt is

considered to be the oldest or original form of money as we understand it in modernity (Graeber, 2011). Debt is inextricably linked to political authority (the threat of violence that prevents the risk of default) and trust (the expectation that debt will, forcefully or voluntarily, be paid). Thus, trust and political authority are considered foundational elements in modern theories of money (note that in cryptocurrency systems, authority is not absent, but instead delegated to technology).

These sociological accounts serve to navigate the complex, ever-lasting question of the relationship between money and value. Why do cryptocurrencies hold value as mere digital data records, which are not recognized as legal tender by legal institutions? What helps here is Derrida's reflection on the feeble distinction between true and counterfeit money. The distinction, he argues, lies in faith: given enough faith, counterfeit money can hold the same value as real money.

The immateriality of money is not a novelty of digital currencies. Amato speaks about money's "irriducibilitá al piano delle cose". This is similarly explained with Marx's metaphor of money as a "universal whore": a token that "negates" the precise content of goods or services, substituting them with a universal, impersonal standard (Giddens, 1990, p. 22).

Even when it circulates as physical banknotes, money performs its function by drawing on its "symbolic force". Its materialization in objects or claims is never a definitive one; its propriety is one of translation, of trans-action: from labor to material goods, from place to place, from present to future, from hand to hand.

This brings us to the conceptualization that is most relevant for the reading of this manuscript, and that is increasingly

useful to understand the ongoing and future evolution of money and value systems as digital objects: money as media. Swartz provides an interesting account of money as a "communication medium dependent on particular technologies" (Swartz, 2020, p. 5).

Payment system / Value transfer infrastructure

If money is media, payment is its communication modality. A payment system, or value transfer infrastructure, is the technology that underpins such communication, enabling value transactions.

Technologies that enable digital value flows are constituted by the cables, data centers, devices, and interfaces that allow the communication of value transfers, which is the recording and authentication of transactions as required by predefined standards of payment settlement[5]. These standards, and the institutions or decision-making mechanisms that define them (the requisites and conditions for a valid payment settlement), are also part of the system.

In digitally native monetary systems, the distinction between money and the technology that underpins it becomes blurred. Digital currency networks are composed of digital tokens (units of value), and the information systems which allow their circulation, from internet backbones to the digital ledgers (software) on which transactions are recorded.

The distinction between the token and the value represented by it is best exposed by the NFT (non-fungible tokens) phenomena. A work of art circulated and embodied by an NFT remains distinct from the token itself. A digital token, therefore, can both be considered the material

5 The 2nd Payment Service Directive defines a *payment system* as a "funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions" (PSD2 Article 4(7)).

representation of money and a part of the technological system which underpins money circulation.

I propose the term *value transfer infrastructure* to overcome the confusing distinction between money, and the media technologies that underpin it, as well as to highlight the focus on the socio-technical assemblages that enable value circulation rather than on the constitution of value itself.

Financial data

Financial data comprises various kinds of personal data generated when financial transactions occur. Transactional data is the information that is necessary for the transfer to be executed, i.e., the amount of funds transferred from x to y. Sensitive payment data is defined by the PSD2 as "data, including personalized security credentials, which can be used to carry out fraud", such as credit card numbers and security codes. Financial transactions, moreover, determine the transmission, storage, and elaboration of a wide variety of personal information that reveal people's localization, purchases, and interactions with people and places.

The aggregation and analysis of these data and the prolonged observation of patterns in financial activities serve to create datasets defined as derivative data. This category of triangulated, elaborated data constitutes the information that is handed over to law enforcement agencies and commercial third parties for risk assessment, customer profiles, and profiling. All this extra information sticks to the transaction data, modulating its value to the extent that whole new industries emerge to capture that value.

(Digital) infrastructure

In this manuscript, the concept of infrastructure is used as a reading lens that imposes a certain critical gaze.

As Star writes, "study an information system and neglect its standards, wires, and settings, and you miss equally essential aspects of aesthetics, justice and change" (1999, p.379). The concept of infrastructure is receiving the attention of Science and Technologies Studies as well as legal scholars interested in digital technologies as it points out the mutual embeddedness of politics and material, technological artifacts.

Digital infrastructures are simultaneously material assemblages and socio-technical processes composed of commercial and institutional relations, cables, digital networks, and devices. They comprise multiple layers of material artifacts, from undersea cables, smartphones, and data centers, to software, standards and settings, entailing precise governance structures, and determining power distribution.

Through infrastructures, normative stances are embedded and transferred upon social and economic exchanges. While appearing as mere technical articulations, they convey political choices, and shape affordances and social practices.

Platform

Platforms have been defined across a variety of disciplines as firms, markets, or data infrastructures. Poell et al. describe them as "(re)programmable digital infrastructures that facilitate and shape personalized interactions amongst end-users and complementors, organized through the systematic collection, algorithmic processing, monetization, and circulation of data" (Poell et al., 2019, p. 3). From a technical point of view, they are technical systems composed of low variability core components on top of which applications can be built, using complementary components. From an economic point of view, "platforms constitute two sided, or increasingly, complex multi-sided markets that function as aggregators of transactions

amongst end-users and a wide variety of third parties" (Poell et al., 2019, p. 7).

Platformization / Payment platform The process of platformization is the "penetration of infrastructures, economic processes and governmental frameworks of digital platforms in different economic sectors and spheres of life, as well as the reorganization of cultural practices and imaginations around these platforms" (Poell et al., 2019, p. 1).

The platformization of payment systems entails the representation of money in the form of digital data (Mejias, 2019) that can be captured and valorized within a platform digital architecture (Sadowski, 2019). It also requires data flows between banks and technology companies, with an outsourcing of intermediation activities from the former to the latter.

There are different models of payment platforms: 1) platforms that position themselves between banks and customers, which are either platforms specialized in payment services (e.g., PayPal, AliPay), or large platforms that integrate payment functionalities within their broader service ecosystem (e.g., Apple Pay, Google Pay); 2) platforms that connect financial infrastructures and businesses, enabling the latter to deliver financial services to customers (so-called Banking as a Service); and 3) platforms that introduce digital tokens as part of their ecosystem (Libra and Commoncoin are examples of tokens meant to circulate within a platform environment).

Blockchain-based digital currencies The core idea of blockchain is that of delegating to a consensus-based protocol, run by a decentralized network of computers, the solution to "the problem of cooperation". It shifts the issue of trust from humans – or human institutions – to a digital infrastructure (thus, to its developers and maintainers). Its stated goal is that

of bypassing untrustworthy, inefficient institutions and allowing individuals to transact with each other in a peer-to-peer manner (Yeung, 2017).

Originating from cypherpunk movements, cryptocurrencies emerged as a solution that proposes to address the issues of trust, transparency, and privacy in financial transactions through technological design. The earliest experiments in privacy-enhancing digital currencies date back to the work of computer science scholar David Chaum. His papers "Blind signatures for untraceable payments" (Chaum, 1982) and "Security without identification: transaction systems to make big brother obsolete" (Chaum, 1985) warn about the threats of the increasing use of electronic banking services to people's freedom and autonomy. Concerned that the "structure of the new electronic payment system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments" (Chaum, 1982, p.1), the scholar – together with his colleagues at the Amsterdam Center for Mathematics and Computer Science – worked on developing a system, based on advanced cryptography and digital signatures, for untraceable electronic payments among pseudonymous users, which would prevent fraud while maintaining users' privacy.

The ideas that are enshrined in Chaum's solution have been significant for the emergence of the Cypherpunk movement (Ramiro, de Quieroz, 2022; May, 1992)[6] , and for further attempts to create anonymous electronic payment systems, such as Hashcash, B-money, Bigold, and finally Bitcoin. The latter – defined as "the first working declination of money intended as a common" (Fumagalli, 2016) – made its appearance on the web through the

6 See: May (1992), The Crypto Anarchist Manifesto, https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html.

mysterious Satoshi Nakamoto's white paper in 2008, and is considered the first application of what we now call a blockchain (Nakamoto, 2008).

Solving the double-spending problem, the Bitcoin protocol underpins a peer-to-peer electronic payment system secured by cryptography, which allows individuals to transact directly with each other without needing third party intermediation.

```
[
  {
    "transactionName": "digitalAssetExists", "transactionLabel": "A test digitalAssetExists transaction",
    "arguments": [ "123456"], "transientData": {}
  },
  {
    "transactionName": "createDigitalAsset", "transactionLabel": "A test createDigitalAsset transaction",
    "arguments": ["123456", "File1", "InvestigationFile", "application_pdf", "10000", "...location/File1.pdf", "ownerID_123",
      "2020-01-01 12:00:00", "1.0.0", "3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8", "subjectID_S_1",
      "categoryID_CAT_2", "Level 1", "Available", "userID_123", "2020-01-01 12:00:00","CREATE"], "transientData": {}
  },
  {
    "transactionName": "readDigitalAsset", "transactionLabel": "A test readDigitalAsset transaction",
    "arguments": ["123456"], "transientData": {}
  },
  {
    "transactionName": "updateDigitalAsset",  "transactionLabel": "A test updateDigitalAsset transaction",
    "arguments": ["123456", "File1", "InvestigationFile2", "application_pdf", "10000", "...location/File1.pdf", "ownerID_123",
      "2020-01-01 12:00:00", "1.0.0", "3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8", "subjectID_S_2",
      "categoryID_CAT_3", "Level 2", "Available", "userID_345", "2020-01-02 16:00:00", "UPDATE"], "transientData": {}
  },
  {
    "transactionName": "deleteDigitalAsset", "transactionLabel": "A test deleteDigitalAsset transaction",
    "arguments": ["123456"], "transientData": {}
  }
]
```


Fig. 4: Example of Transaction Data File from IBM Blockchain Platform extension of Visual Code Studio (Source: Leite, Albuquerque, Pinheiro, 2020).

1.3 PROBLEM STATEMENT AND RESEARCH QUESTIONS

This manuscript explores different ways in which the development of digital value transfer infrastructures is influenced by – and contributes to – processes of legal change and redistribution of power across various geographies and scales. This general problem is addressed through four research questions.

Question 1: The issue of privacy has been the starting point of my reflection on how normative goals are achieved both by means of technological design and through systems of legal protection.

Digital payment infrastructures are populated by digital service providers with data-intensive business models. Financial data is increasingly part of the data economy. Because of its relevance to law enforcement and public administration, however, financial data enjoys a special status compared to other categories of personal data. Requirements of data collection and retention imposed by sectorial financial regulation compromise some of the data protection principles enshrined in the GDPR (Frasher & Agnew, 2016).

The trends that technology companies are introducing in the financial industry and its data practices (e.g., the commercial exploitation of financial data, the international dimension of financial informational networks, and the use of automated processing and decision-making tools) urge us to address questions related to the consequences that the digitalization of the financial infrastructure raises in terms of privacy, data protection, and the geopolitics of data governance (Amoore & de Goede, 2021). Therefore, the first question I deal with is:

What consequences do practices of financial data monetization have in terms of privacy and data protection? Are the European legal instruments aimed at protecting privacy adequate to deal with ongoing transformations in digital value transfer infrastructures?

Question 2: As a reaction to increased financial surveillance and a lack of trust in financial institutions,[7] decentralized blockchain systems allow confidential transactions by enabling recordkeeping and value circulation without identification, and by removing central points of control.

Notwithstanding the initial reluctance to interact with the legal system, the evolution of the blockchain industry has been highly influenced by the related legal responses. As the latter varied from complete opposition (for example in China) to more friendly approaches (in Malta, Luxemburg, etc.), crypto-assets-based ventures were at times adapting to comply with, and at times trying to escape, applicable legal regimes.

7 Rooted in open-source cultures, the rise of blockchain-based financial networks expresses a neo-libertarian response to the post-2008 crisis of trust in political and financial institutions. Among the speculations on what this technology could deliver is the belief that it can nurture new, horizontal socio-economic organizations and help increase transparency in institutional processes.

The development of the industry shows, on the one hand, that legal obligations created incentives for the reorganization of activities around incorporated businesses. On the other hand, the strengthening of law enforcement activities over cryptocurrencies' networks motivated further experiments in less detectable, less reachable transaction systems, deploying "mixers"[8] or other obfuscation techniques to hide users' identities.

The development of cryptocurrency projects illustrates, therefore, the cat-and-mouse dynamic that takes place in the co-evolution of digital infrastructures and legal systems, offering a broader understanding of the dynamics that govern the co-evolution of digital infrastructures and the law. By discussing law enforcement and regulatory activities in this domain, I address the following question:

How do dynamics of legal change and law enforcement influence the development of digital infrastructures? In turn, how is legal change influenced by continuous updates in technological design?

Question 3: Whether the goal is to restrict the use of unregulated cryptocurrency networks, constrain the power of large technology companies, or mobilize the construction of digital infrastructures as public utilities, policymakers are guided by certain imaginaries of what the future of digital money and payment infrastructures should look like.

The concept of sociotechnical imaginaries (Mager & Katzenbach, 2020; Jasanoff & Kim, 2009) – shortly introduced in the theoretical framework and further explained in Chapter 4 – is crucial to understanding the co-development of legal and technological systems in light of the discourses[9] that shape them.

Just as coexisting digital money infrastructures develop on different planes and along different lines, European policy produces responses and strategies

8 In cryptocurrency communities, a mixer is known as a technology that shuffles transaction entries in order to hide the connection between the users initiating the transactions and the transferred funds.

9 Discourse is intended in the Foucauldian conception, as a historically contingent system of meaning, composed of language, ideas, and values as conveyed by dominant disciplines and institutions, and translated into societal practices.

that pursue various, at times conflicting goals. Moving from one sector of policy to another, incongruences emerge in the legal goals and produced effects of regulation. For example, if on the one hand the GDPR imposes data minimization and careful sharing agreements among companies and institutions, on the other hand the PSD2 forces banks to open their databases to data-intensive technology businesses.

EU regulators favor the entrance of technology companies in the financial services sector, aiming to advance digitalization and innovation. This strategy seems to be at odds with other measures taken by EU regulators to prevent or mitigate the risks raised by the expansion of bigtech platforms across the EU in multiple sectors of the economy. To address this ambivalent attitude of policymakers in the analyzed domain, I formulate the following research question:

Which sociotechnical imaginaries of digital payments underpin the EU policy agenda on fintech? In particular, which notion of consumer interest is mobilized to justify the choices enshrined in the policy agenda?

Question 4: Against the background of a digital payment and digital currency industry that threatens to undermine institutions' ability to exercise their monetary power (Pistor, 2020) and law enforcement functions, initiatives are being developed to build digital money infrastructures as public utilities, re-establishing a link between money and institutionally-defined places or communities.[10] These initiatives, attached to particular imaginaries, understand the capacity of money to organize and define social relationships, and the need to advance socio-political considerations concerned with the public interest in the construction of crucial infrastructures.

Identifying the appropriate "place" of money (Amato, 2016; Muellerleile, 2020) is to identify the scale and geographies of the infrastructures through which it flows. In opposition to increasingly de-territorialized and de-institutionalized digital infrastructures, public institutions are proposing possible localities around which a notion of *public* and *public interest* can be drawn. As these

10 The scenario of government-led digital infrastructures is best exemplified, in the domain of digital money, in the proposals for and experimentations with Central Bank Digital Currencies.

initiatives differ among each other in terms of scale, socio-political goals, and technological design, my analysis addresses the following question:

What is the relationship between scale, socio-political goals, and technological design in digital value transfer infrastructures built as public utilities?

1.4 STRUCTURE OF THE MANUSCRIPT

The articles collected in this manuscript explore three coexisting types of digital money infrastructures: a) decentralized blockchain-based networks of value circulation; b) payment networks organized by and around commercial digital platforms; and c) public digital money infrastructures. The four papers included in this thesis deal with four interconnected, traversal issues discussed in relation to these three models of digital infrastructures: privacy, law enforcement, sociotechnical imaginaries, and scale. The selection of papers covers only some of the conjunctions between the identified issues and the use cases (as schematically indicated in Table 1), yet the findings and discussions provided by each chapter offer tools to think critically about these issues in a traversal manner, beyond the case to which they are referred to in this manuscript.

	Decentralized networks	Commercial digital platforms	Institutional digital infrastructures
Privacy	5	2	5
Law enforcement	3	2	2
Sociotechnical imaginaries	5	4	4,5
Geography	5	2	5

Table 1: Conjunction of problems and use cases in the manuscript's chapters.

1.5 THEORETICAL BACKGROUND

1.5.1 PRIVACY IN FINANCIAL INFRASTRUCTURES

As we pay through digital devices, money loses its materiality and circulates as information expressed as data, binary codes, and signals generated electronically on circuit boards.

The digitalization of monetary flows allows capillary systems of financial surveillance to be organized that – exceeding previously conceivable levels of efficiency in transaction monitoring – serve multiple purposes, from law enforcement to consumer profiling for marketing and credit risk assessment (Hildebrandt, 2009; de Goede, 2011).

The disappearance of cash, and the exclusive use of digital transaction systems – whether these are commercial payment platforms or Central Bank Digital Currencies – would compromise "any notion of maintaining anonymity and privacy in financial matters" (Prasad, 2021, p. 22).

Financial transaction data is highly intertwined with public power and law enforcement (Lauer, 2017; Scott, 1998), as it is used to detect illicit activities such as tax evasion, money laundering, and terrorist financing. Such data is also highly valuable in the context of data-intensive commercial practices, as they are revealing of individuals' activities, employment conditions, purchases, geographical movements, and so on. The dual use of financial information in law enforcement processes and for commercial purposes creates a legal gray area of lowered privacy protection.

The analysis provided in Chapter 2 explores how the tension between these two priorities – privacy and law enforcement – in the governance of financial data is played out in European legal frameworks, analyzing the legal instruments that apply to financial information: the General Data Protection Regulation, the Law Enforcement Directive, the 5th Anti-Money Laundering Directive, and the 2nd Payment Services Directive.

The geopolitics of financial data governance is an urgent object of study, which cannot be understood in isolation from a broader understanding of the expansion of global technology platforms in all sectors of the economy

(Westermeier, 2019). Privacy in financial transactions, in fact, is ever more relevant as the intermediation of payment services is taken over by technology companies based in countries with lower levels of privacy protection (PayPal, Google Pay, Apple Pay). This has direct consequences in terms of privacy: companies located abroad have law enforcement-related obligations toward their national authorities, from which derives the potential transmission of data of European citizens to governments and law enforcement agencies in countries with lower standards of privacy (a practice to be assessed in light of the Schrems II judgment).

Moreover, the fintech domain offers interesting examples of how absolute transparency and reduction of human arbitrariness in decision-making bring about risks of discrimination, denial of privacy, and exclusion of those who deviate from the normative majority. Following the logics of actuarial justice and risk-based regulation, the sub-derivative data that constitute financial profiling are involved in automated decision-making processes of financial intelligence, as well as credit allocation and marketing strategies.

Personalized pricing, robot advice, and algorithmic decision-making on the most disparate issues such as granting a loan or a rental contract are based on systemic and intentionally discrimination practices (Borgesius & Poort, 2021); they are designed to judge based on intersecting pieces of information, finding differences and signaling *errors*, such as when a resident permit is missing, when data about gender does not coincide with data about sex, or when countries of origin are blacklisted (Guyan, 2022) [11].

Not surprisingly, privacy in financial transactions is one of the core issues around which the negotiations and contestations addressed in this thesis evolve; moments of rupture and convergence among the imaginaries and architectures analyzed in the following chapters are determined by the definition of identification standards and subsequent privacy *settings*.

The tension between privacy and law enforcement is core to the development of decentralized cryptocurrency systems, from their origins in cyberpunk cultures to their co-evolution within specific regulatory frameworks. In

11 Several scholarly works have exposed the intrinsic discriminatory nature of algorithmic systems. See, for example: Eubanks, 2017; O' Neil, 2016; Noble, 2018; Guyan, 2022.

blockchain-based networks, in fact, decentralized data storage, processing, and validation are design choices meant to avoid issues of confidentiality and privacy intrusions by centralized third parties:

> *Centralized systems can be transformed into decentralized systems both in order to eliminate the single point of failure in terms of availability and to reduce the risk to this trusted party of being coerced to harm privacy* (Musiani et al., 2016, p. 16).

Privacy also remains a core value in the development of digital money infrastructures by European institutions. The first report issued by the ECB about a potential European Central Bank Digital Currency, which was published in December 2019 and titled "Exploring anonymity in Central Bank Digital Currencies", describes a proof of concept for a payment system in which, thanks to distributed ledger technology, AML/CFT-compliance procedures are carried out without central banks or other intermediaries having visibility on user identities, thus preserving privacy while ensuring law enforcement procedures (ECB, 2019). As Chapter 4 exposes, however, there are other interests guiding policymaking in the field of digital payments. The platformization of the ecosystem, and the inability or unwillingness to cut out technology companies as identity providers, hamper efforts to create truly anonymous, peer-to-peer, privacy-preserving transaction systems.

1.5.2 LAW ENFORCEMENT AND DIGITAL INFRASTRUCTURES

The alleged anonymity of peer-to-peer digital value transfer infrastructures was the starting point of regulatory efforts aimed at bringing the cryptocurrency industry under supervision and law enforcement reach. This was expressed both with the amendment of the 5th AMLD[12] and with the proposed adoption of the MICA regulation.[13]

12 This amendment establishes that AML rules apply to "providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers". *Obliged entities* are required to: perform customer due diligence (identification of customers) on transactions, and send reports to the Financial Intelligence Unit in case of suspicious transactions, under the supervision of the AML Supervisor.

13 This regulation seeks to provide legal clarity on the regulatory treatment of crypto-assets that are not covered by existing financial services legislation; support innovation and fair competition; instill appropriate levels of consumer and investor protection and market integrity; and ensure financial stability in the crypto-assets ecosystem.

Blockchain was born as technology meant to protect its community of users from governments' interactions and violations of transactions' confidentiality. The technology is explicitly designed to prevent unilateral censorship and privacy intrusions. The spread of cryptocurrencies and blockchain-based technologies, therefore, has given renewed attention to the possibility of coding to underpin alternative modes of societal self-organization and rule enforcement. The entire blockchain saga is built on the mantra of "code is law", i.e., the idea that code can function as a substitute to law in the ordering of social systems (Goanta & Hopman, 2020). *Decentralization* enjoys an almost mythical status in the discourses around blockchain, and is considered the key feature allowing interference from external enforcement to be avoided, and horizontal self-regulation to be organized.[14]

The decentralization of the nodes running distributed ledgers' transaction systems, however, did not prevent the consolidation of a service layer industry centralized around legally responsible market actors. Centralized crypto-exchanges, hosted wallet providers, and NFT marketplaces started acting as intermediaries among users and underlying software components; as these intermediaries perform regulated activities, they reintroduce law enforcement and compliance in a system that was designed to circumvent it.

The development of regulated markets of crypto-assets and related services was yet another demonstration that the re-centralization of a decentralized techno-social system is produced by both markets and regulatory frameworks. Laws move ventures geographically, cluster them within more favorable jurisdictions, and modify their business models through both punitive and incentive systems.

---

14 In blockchain discourse, decentralization mostly refers to the decentralization of the software components, i.e., the storage and maintenance of the digital databases, the validation of transactions, and the implementation of changes in the software. However, there are multiple layers in a complex techno-social system which determine the distribution of architectural, political power below and above the software. According to Buterin (2017), decentralization in the software layer implies decentralization in the following dimensions: (1) Architectural (e.g., the physical distribution and number of computers running a system); (2) Political (e.g., Who controls such computers? How are changes in system implemented?); and (3) Logical (If you cut the system in half, including both providers and users, will both halves continue to fully operate as independent units?). According to this classification, "Blockchains are politically decentralized (no one controls them) and architecturally decentralized (no infrastructural central point of failure) but they are logically centralized (there is one commonly agreed state and the system behaves like a single computer)"(Buterin, 2017).

At the same time, however, legal responses to blockchain financial systems also produced further waves of law-avoidant technologies designed to resist re-centralization, de-anonymization and regulation. The strengthening of law enforcement activities over cryptocurrencies' networks motivated experiments to create less detectable, less reachable transaction systems managed by legally unreachable, dispersed groups.[15] Decentralized exchanges, known as unhosted wallet providers, function without a liable intermediary; mixers and tumblers prevent the traceability of transactions and their relatability to individual users.

The history of blockchain ecosystems, therefore, situates itself in a continuation with the history of the Internet as a history of networks that try, by means of technological decentralization, to avoid regulation, surveillance, or censorship, and recurrently recentralize around regulated intermediaries due to their inability to exist without some forms of institutional endorsement (Bodó & Giannopoulou, 2019).

If on one end of the spectrum there are decentralized techno-social systems that jeopardize regulatory efforts by dispersion of controlling nodes and identifiable actors, on the other end there are centralized technological ecosystems that pose equally compelling law enforcement issues. While being demanded by regulation to design technological systems in compliance with normative frameworks, in order to prevent copyright infringements or hate speech,[16] for instance, large digital platforms circumscribe areas of digital activity where they define and enforce their own, customized sets of rules (Helberger, 2006), effectively exerting forms of digital sovereignty[17] within their own ecosystem (Bratton, 2016).

Incentivized by liability schemes, platforms embed rules for access, censorship schemes and tracking programs in their technological systems, thereby assuming

---

15 These solutions mainly fall into the categories of decentralized exchanges and so-called unhosted wallet providers, which is software or hardware which store cryptocurrencies on behalf of users, without holding funds or private keys.

16 For instance, the concept of *privacy by design* enshrined in the European General Data Protection Regulation requires *data controllers* to design their technological system as to ensure the protection of the rights set out by the Regulation.

17 On the concept of *digital sovereignty*, see: Pohle & Thiel, 2020.

policing functions traditionally attributed to public agencies. The regulation of platforms[18] becomes ever more problematic the more they become *infrastructures*, similar to the railroad, telephone, and electric utility monopolies of the past century. By forging "both computational *and* economic connections with complementors, such as content developers, businesses, content creators, and advertisers" (Poell, Nieborg, van Dijck, 2019, p.4), platforms position themselves at the center of larger Internet economic and data infrastructure (Fathaigh, van Hoboken, van Eijk, 2019). Hence, the delegation of law enforcement duties to these giant intermediaries further enhances their powers exercised through data control, behavioral manipulation and market dominance.

Platforms' sovereignty became a matter of financial and monetary power when, in 2019, Facebook announced its plan to issue a fast-scaling, global digital currency based on blockchain technology: Libra. The currency would enable Facebook's users to transfer money *in app* from account to account, and to other e-commerce platforms. The payment system would have been controlled by a single entity, the Libra Association, whose legal structure was designed to shield its members from the liabilities that apply to financial institutions (Pistor, 2019). Given the geographical dispersion of the Libra governance structure,[19] and the global dimension of its customer base, national jurisdictions would be in competition with each other and likely fall short in their attempt to regulate the functioning of the currency.

Decentralized cryptocurrencies on the one hand, and the Libra project on the other, are both examples of digital money and payment infrastructures that develop in opposition to, or simply outside of, national monetary sovereignty. They both challenge governments and law enforcement capacity to control financial flows and pose questions regarding the negotiation powers of institutions vis-à-vis large-scale, techno-social systems of value creation and distribution.

The modalities and extent to which regulatory powers allow or compress spaces for these diverse techno-social systems to develop depend on perceived

18 On the concept of platformization: Poell, Nieborg, van Dijck, 2019.

19 The initiative is led by Facebook Inc., incorporated in the U.S.; however, the Libra network is officially governed by the Libra Association, a non-profit entity established in Geneva. The Association, in turn, is composed of corporations and organizations that, located in various jurisdictions, will act as nodes of the Libra blockchain.

threats, expected benefits and, ultimately, narratives and imaginaries about the future of money that regulators consider foreseeable.

1.5.3 SOCIO-TECHNICAL IMAGINARIES IN POLICYMAKING

Making policy involves prospecting possible futures and acting toward their materialization. Images of the future are co-constructed by discourses, narratives and ideals that are influenced by a variety of actors. Lobbying, marketing, material artifacts, institutions, political movements, and counter-movements all contribute to building coexisting socio-technical imaginaries of what the future might look like.

The concept of socio-technical imaginaries has become crucial to understand processes of digital transformation and the legal changes which accompany them. Drawing upon the literature on this concept, the articles of this thesis understand the construction of digital money infrastructures as the materialization of policy choices, economic interest, ideologies, and myths that are produced and pushed by different groups – institutions, technology companies, digital activists, or scammers.

The concept of socio-technical imaginaries (Mager & Katzenbach, 2020; Jasanoff & Kim, 2009) is deployed and explained in Chapter 2, which explores the discourse that guides the European policy on digital payment infrastructures. The point of this chapter and its function in the context of this manuscript is to illustrate, on the one hand, that there are multiple, coexisting, and contested visions of future digital payments, and on the other, that the consolidation and materialization of such visions is dependent on meeting the interests of different stakeholders. In our case, analyzing a policy that promotes privatization and platformization of digital payment, we understand the role of technology companies in shaping visions about the future, and directing institutional activity in its materialization.

Located in the broader context of this thesis, this chapter highlights the limitations of a policy approach that puts blind faith in a certain narrative of technological development. Digital payments, according to the dominant imaginary that permeates the agenda, must be fast, seamless, cross-border, and cheap, and they need to make use of cutting-edge technologies such as

data analytics and AI for personalized and optimized experiences. Alternative visions of money and payments, such as slow, hard-to-use, privacy-oriented cryptocurrency systems, or community-based exchange systems, as well as the legal and societal issues that are implied by platformization, are – either for convenience or due to narrow-mindedness – left aside.

Chapter 5 highlights how each vision of future technologies is accompanied by an idea of public and individual interest (Lynggaard, 2019). This idea of public interest mutates with the discourse: it reflects the goals and interest of the given group, institution, or market player that produces them (Mak, 2015).

Policymakers depict, at times, users of digital technologies as passive receivers: they justify a liberal approach to the digitalization of financial services under the belief that better technologies will serve the public interest, subscribing to a rhetoric of users' technological empowerment. These assumptions can be criticized in light of the findings of Chapters 2 and 4, which highlight issues of privacy, consumer protection, and threats to individual rights posed by these supposedly empowering technologies, while offering alternative views of what the goals and socio-political premises of digital money infrastructures might be.

1.5.4 THE SCALE OF DIGITAL INFRASTRUCTURES

Due to a rhetoric of "trustworthiness" (Bodó, 2021), blockchain technologies have stimulated a wide variety of experiments in the public sector, mostly consisting of the creation of decentralized infrastructures for public data management, auditing, and recordkeeping.[20] Pilot projects are proliferating among governments and municipalities. For example, the DECODE project – funded by the EU Commission and currently being piloted in Amsterdam and Barcelona – is testing the use of blockchain to build an open architecture

20 What Karen Yeung (2018) names the *efficient alignment* between technical code and legal code is the foundational idea of what is commonly referred to as *regtech*: technologies built to streamline auditing and enforcement of substantial legal requirements. The rhetoric that underlies the creation of technological infrastructures for legal procedures and administrative data management is anchored to the idea of technological efficiency and trustworthiness. Trust is the central problem tackled by the discussion about technological implementations in the public sector. The reason for blockchain's hype and success among policymakers is exactly its supposed suitability for the resolution of the trust issue.

for the management of citizen data. The aim is to build a system that allows a high standard of privacy, individual control over personal data, and open data pools.

Chapter 5 presents three EU-funded projects which involve the creation of digital value transfer infrastructures at different scales of institutional power and geographical extension: the Commoncoin, meant for geographically sparse, self-organized communities; the digital euro, meant to work as the official digital currency of the eurozone; and the REC, circulating in the Municipality of Barcelona.

All three projects are initiatives intended to explore the construction of blockchain-based digital currencies under the control of public institutions or citizens' organizations. These emerging – experimental or speculated-about – digital value transfer infrastructures do not follow the same geographical borders, or the same institutional logics of value circulation, of traditional, state-centered monetary systems.

Money's symbolic force is derived from, and is dependent upon, institutional relationships, communitarian conventions, or exercises of sovereignty. As an emblem, its legitimation and functioning is connected to an institutionalized sovereignty, or circumscribed community, and therefore to a specific "place" (Amato, 2016). However, not only the sovereignty and the community, but also the place of money differs, as multiple digital value transfer infrastructures coexist at different scales and across different virtual and territorial localities.

As the adoption of the euro at a supranational scale has demonstrated, monetary spaces can be super-imposed across territories to enforce financial, political, and economic interdependence. This super-imposition can re-shuffle the sense of community and perceptions of territorial union, and affect the political agency of groups and institutions, as the latter relate differently to these value systems and their material, institutional (infrastructural) underpinning.

In "The Consequences of Modernity", Giddens analyzes money as one of the fundamental "symbolic tokens" that are responsible for the "disem-

bedding of social systems" in modernity. By "disembedding", he means the "'lifting out' of social relations from local contexts of interaction and their restructuring across indefinite spans of time-space" (Giddens, 1990, p. 21). Money is a vehicle through which institutional and social relationships, as well as power, are dynamically *deterritorialized* and *reterritorialized* (Delauze and Guttari, 1972), moved among political institutions and markets, from local communities to global actors (de Goede, 2020), across networks "of variable geometry and dematerialized geography" (Castells, 1996, p. 359).

A similar form of geographical distortion is determined by digital technologies. As they are simultaneously local and global, and national and international (Bernards and Campbell-Verduyn, 2019), they bundle together geographically sparse "places", create new virtual "localities", and shuffle communities.

Digital value transfer infrastructures link to communities of varying dimensions and geographical distributions, not identified by territory or jurisdiction but by conditions of access, digital literacy, and resources. A central question in the construction of such infrastructures, therefore, is what "places" and communities they serve: the "locality" traced by the infrastructure, which is intrinsically related to its social and institutional underpinning, and the political visions and societal goals that are embedded in it.

Defining "scale" (LeFebvre, 1974; Castells, 1996) not merely as geographical dimensions, but also the conditions for inclusion in and exclusion from the digital infrastructure, I deploy this concept in Chapter 5 to frame considerations about governance, socio-political agendas, and technological architectures of emerging (speculative) digital infrastructures of value flow.

1.6 RESEARCH METHODS

When a technology or technological phenomena becomes the focus of academic research, multiple possible paths, questions, and analytical tools present themselves to the researcher. The choice among these paths depends, partially, on speculation: about which applications will be relevant in the future, which legal frameworks will be activated, and which industries, processes, and rights enforcement systems will be threatened. This kind of speculation involves considerations that are from legal thinking. Can we, as lawyers, as

social scientists, as philosophers, predict the evolution of rapidly changing socio-technical developments? Which activities will be relevant? Which actors? To what extent will hyped technologies (think of the regulatory craze around AI) really be relevant for regulators?

1.6.1 POSITIVE LEGAL ANALYSES

The parts of this dissertation which consist of doctrinal legal analyses are not aimed at providing an exhaustive analysis of privacy regulation in the financial domain, or of the financial regulation of cryptocurrencies. Rather, their aim is to highlight how certain socio-technical developments make old laws obsolete, unenforceable, and not fit for purpose under new configurations of technological infrastructures. The assessment of the clash between the static legal framework and the changing technological infrastructure is a necessary point of departure for further inquiries about broader interactions between legal systems and technological infrastructure in their relationship and mutual influence.

The problem of the identification of the "right" legal framework is a problem without a stable solution. The selection and analysis of a given legal framework serves to operationalize legal rules and stress-test the legal system against technological artifacts and code-based modes of organization. The choice of the legal framework is made by assessing the activities of regulators and the discussions on academic and online forums about technological and legal developments. A relevant part of this type of research consists, in fact, of understanding which parts of the legal system get "activated" by a given socio-technical phenomena. In the case of cryptocurrencies, it was clear that, at the time of writing, the qualification of crypto-assets under finance law – and the subsequent possibility to regulate financial activities, e.g., what are known as ICOs, involving blockchain-based digital tokens – was the main topic of discussion within European institutions and among industry actors.[21] It was also the domain which allowed concrete law enforcement cases to be discussed. Therefore, observing how the issue unfolded was key to addressing broader questions about the relationship between decentralized financial technologies and regulation.

---

21 This intuition was later confirmed by the adoption of the MiCA regulation.

New technological developments may give rise to social, economic practices which fall under the purview of multiple, possible regulatory regimes, and oftentimes it is not known which framework will be the fastest, most useful, effective, and enforceable to tackle the issues. In the regulation of the value transfer stack, the GDPR, financial legal frameworks, and criminal law could all play a role: that financial regulation turned out to be the area with the most activity on cryptocurrencies was the product of a number of accidents, as much as the agility of authorities in this domain.

The question of the right legal framework is also not one that urgently needs answering. What I am observing is a regulatory war between different institutional powers trying to experiment with the right legal responses, pursuing various objectives at the same time, changing such objectives over time (attracting cryptocurrency-related innovation, banning cryptocurrencies, contrasting the power of bigtech platforms, etc.) following non-linear and contested political agendas. So rather than focusing on one, I decided to observe the dynamics of institutional responses with a broader gaze. In this way, I aimed to produce research that can be relevant beyond the domain of activities and the fields of law with which it deals.

1.6.2 EMPIRICAL METHODS: DISCOURSE ANALYSIS AND INTERVIEWS

I have, then, deployed various methodologies aimed at understanding not only the mechanics of how rules apply to technological applications, but also the processes around policy assessment, policymaking and infrastructural development in the domain of digital money.

I found discourse analysis of policymaking to be the most suitable tool at my disposal to unpack the imaginaries and discourses which inform legal change in the construction of digital payment infrastructures. Discourse analysis is deployed to study the sociotechnical imaginaries in policymaking on digital payments, which in turn allow a reflection on how such policymaking responds to narratives and incentives that merge public interest with the interests of the private technology sector.

As opposed to fast-changing techno-social actors and artifacts, institutions are "by definition the more enduring features of social life" (Giddens, 1984, p.24). As "collectively accepted" formal organizational structures, institutions embody collective values, discourses, and systems of meanings that shape particular views of the world, and of the future. Understanding the discourse that is legitimized and crystalized in institutional practices and decision-making is even more important when studying institutional approaches that are future-oriented. The policy on digital payment infrastructure analyzed in Chapter 4 is a story about a future to be built, and a set of prescriptions for its realization. The policy conveys "concretely constructed" imaginaries that, when "institutionally stabilized" and promoted, become performative as they induce the materialization of technoscientific projects. This therefore involves questioning such policy demands, retracing how such imaginaries and narratives have formed, under which incentives they have been chosen over others, and which actors and stories have contributed to their consolidation.

While software-assisted textual content analysis[22] proved useful to deconstruct and criticize the EU's policy agenda on fintech, a more direct engagement with the developers, activists, policymakers and experts felt necessary when inspecting the actual construction of digital payment infrastructures in Chapter 5. Hence, I decided to conduct in-depth expert interviews as a way to explore the goals, and political and technical choices that underpin infrastructural projects for payment infrastructures in Europe. This choice was, in all honesty, motivated by a lack of alternative options: as the digital euro, REC and Commoncoin are experimental, highly technical as well as highly political projects, no sources were available providing a comprehensive and honest overview of the intention, technical details, and governance mechanisms underlying them.

22 On the use of content analysis software in legal research, see: Schebesta, 2018.

1.6.3 THE GLOSSARY OF DECENTRALISED TECHNOSOCIAL SYSTEMS

Critical thinking in universities often develops along the lines of sector-specific concepts, problems, and terminologies. Academic research in social sciences, in particular law, is anchored to methods and fields of inquiry that, to achieve simplification and soundness, leave aside aspects of the problem that are dealt with by other disciplines.

The meaning of concepts and terms are, however, co-created, contested, and continuously renegotiated by multiple voices. When the object of study is in flux, the terminology is constantly outdated; concepts need to change with a speed that academic research cannot sustain. With a highly ideological charge, discourses on decentralized technologies have generated a wide vocabulary of context-specific terms that associate political, societal, and technological issues in rather original ways. Just as any other subject, however, these technologies (as tools, as conceptual design, and as symbols) are rooted in specific geographies, ideologies, and gender relations, and reflect the biases encoded in these contexts. The related terminology is used and interpreted according to different purposes and preconceptions and/or misconceptions. This prevents fruitful confrontations on these types of technological developments, paving the way to uninformed hypes and prejudices among scholars and public institutions.

The challenge of learning, understanding, and clarifying contested terminology, the definition of which required expertise from various domains, has been partially dealt with through the curation of the Glossary of Decentralised Technosocial Systems, to which I contributed throughout my Ph.D. as chief editor. The idea of the Glossary arose from this need for a workable, yet flexible and multidisciplinary resource for terminological clarity, which reflects instead of denying complexity. This editorial project is thought of as an academic research toolkit that, by asking for contributions from interdisciplinary teams of researchers, maps how meaning and terms evolve and change across disciplines, times, and geographies.[23]

---

23 See: Ferrari, 2021, Glossary of Decentralised Technosocial Systems.

Gathering information overlaps with its production, with the involvement of those experts who are in a position to represent or report about the use and evolution of complex terms. Rather than giving definitive and crystalized answers about meaning, the Glossary is interested in tracing the negation behind its enduring construction and evolution, illuminating the power of multiple discourses and practices that compete in its definition.

1.7 OVERVIEW OF THE THESIS

Chapter 2 explores the data practices – and their consequences in terms of privacy – of digital value transfer intermediaries, as the banking sector and the digital payment industry enter the data economy. Financial data are key to various law enforcement processes, including criminal investigations, anti-money-laundering strategies, and the implementation of national fiscal policies. However, financial data also qualify as personal data. While law enforcement objectives can derogate from certain privacy-related legal safeguards, private financial firms should, in principle, comply with the privacy standards upheld by the GDPR. Highlighting the most critical trends of the current financial industry (i.e., commercial exploitation of data, international dimension of financial informational networks, and use of automated processing and decision-making tools), the chapter analyzes how privacy and law enforcement priorities interplay in determining the governance of financial data. It concludes by recognizing that privacy loopholes exist in the current financial industry's data practices, and that, as payments tend to be increasingly performed digitally, thus exponentially increasing the availability of financial data, privacy-enhancing payment methods should be encouraged and legitimized. (The chapter is based on *Ferrari V. (2020) Crosshatching Privacy: Financial Intermediaries' Data Practices Between Law Enforcement and Data Economy. European Data Protection Law Review,* reproduced here with minimal changes)

By analyzing the guidelines issued by the European Securities and Market the legal qualification of blockchain-based crypto-assets under EU law. Focusing on crypto-assets that function as a) investment instruments (that is, investment tokens), and as b) electronic money (that is, payment tokens), the work outlines shortcomings and drawbacks in the applicability and enforcement of existing EU legal frameworks regulating investment activities

and payment services. The conclusion elaborates on the relationship between law enforcement, regulatory intervention, and socio-technical developments in the crypto-assets' ecosystem. (The chapter is based on *Ferrari, V. (2020). The regulation of crypto-assets in the EU – Investment and payment tokens under the radar. Maastricht Journal of European and Comparative Law,* reproduced here with minimal changes)

Chapter 4 investigates, through a qualitative analysis of official documents, how certain imaginaries about technology filter into EU policymaking, allowing or accelerating the trans- formation of payment infrastructures into the platform economy. One of the ways in which socio-technical imaginaries filter into policymaking is, it turns out, by informing an image of the consumer which serves to justify measures for the realization of a desired future. In particular, the documents offer a view of the consumer as an actor that is empowered by digitization. The thesis proposed with this chapter is that this view of the consumer is partial: the rhetoric of consumer technological empowerment outweighs and conceals much-needed considerations about the vulnerability of consumers vis-à-vis data-intensive payment technologies. Ultimately, the fault lies with the future imaginaries upon which such an image is grounded. The vision of the digital payment infrastructure portrayed in the documents is in fact problematic for two reasons. First, the technologies that are portrayed as desirable are chosen based on industry interests and trends, rather than considerations of the benefits and risks that these technologies entail. Secondly, the assumption that a liberalized market will offer more and better choices is flawed, as platformization entails risks of monopolization and abuses of market power. The chapter suggests that policymakers in this domain should be more critical of the risks entailed by platformization, and open their imagination to alternative technological futures (The chapter is based on *Ferrari V. (2022) The platformisation of digital payments: The fabrication of consumer interest in the EU FinTech agenda, Computer Law & Security Review,* reproduced here with minimal changes).

Chapter 5 is concerned with investigating the relationship between scale, socio-political goals, and the technological design of digital money infrastructures. Against the background of a digital currency industry that undermines

institutions' monetary power, institutions are developing digital money infrastructures conceived as public utilities. Taking place at different scales, the coexistence of digital currency projects within the EU opens questions about the proper "place" of money in digitized societies. Using interviews, the chapter explores three publicly-funded projects that organize digital money infrastructures at different scales. By comparing the latter, it emerges that smaller scale and bottom-up governance means greater attention for local problems and social dynamics; however, links to institutions and top-down decision-making remain necessary to ensure long-lasting and scalable digital money infrastructures. (The chapter is based on *Ferrari V., Chiappini L. (2023) Digital geographies of power: The scale of digital money infrastructures, forthcoming*, reproduced here with minimal changes).

Chapter 6 draws the general conclusions. Grounding the criticism of the legal construction of privacy on the political economy of the actors that organize digital commerce and information flows, the conclusions of this manuscript invite academics and regulators to widen their imagination to alternative possible futures of digital infrastructures. It advocates the acceptance of imperfection as opposed to *perfect targeting* and *perfect enforcement*. It welcomes the rise of multiple, contested, delocalized and vertically overlapping digital value transfer infrastructures, as they express the prerogatives of different groups – social, economic, and political actors. It suggests, ultimately, that plurality is a necessary antidote to the totalizing effects of surveillance apparatuses enabled by datafication and algorithmic enforcement. It argues that the possibility of an "outside" in the landscape of potential digital architectures needs to remain imaginable and designable. For this reason, in the co-development of legal systems and digital infrastructures that are core to public life, conflicts are productive. Negotiations, ruptures and exceptions are constitutive of the unending process of mutual reinforcement, and mutual containment, in which a plurality of agencies – expressed through legal institutions, symbolic systems, as well as information and media structures – are entangled.

The thesis is composed of the following articles:

Ferrari V., Chiappini L. (2023) Digital geographies of power: The scale of digital money infrastructures, forthcoming: First Monday, Governance by Infrastructure Special Issue. (Letizia Chappini has contributed to build the theoretical framework, regarding the geography of digital infrastructures, and assisted the empirical work. Valeria Ferrari conducted the interviews and wrote the entire article).

Ferrari V. (2022) The platformisation of digital payments: The fabrication of consumer interest in the EU FinTech agenda, Computer Law & Security Review, Volume 45, 105687, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2022.105687.

Ferrari V. (2020) Crosshatching Privacy: Financial Intermediaries' Data Practices Between Law Enforcement and Data Economy. European Data Protection Law Review, 6(4), 522-535.

Ferrari, V. (2020). The regulation of crypto-assets in the EU - Investment and payment tokens under the radar. *Maastricht Journal of European and Comparative Law*, *27*(3), 325-342.

Other published works that form part of the analysis informing the thesis are:

Ferrari V. (2020) Tecnologie e geografie di potere delle piattaforme digitali: Libra. Kabul Magazine. https://www.kabulmagazine.com/tecnologie-geografiei-potere-piattaforme-digitali-libra/.

Ferrari V. (2021). Introducing the glossary of decentralised technosocial systems. Internet Policy Review, 10(2). https://doi.org/10.14763/2021.2.1546.

Giannopoulou, A., & Ferrari, V. (2019). Distributed Data Protection And Liability On Blockchains. In S. S. Bodrunova, O. Koltsova, A. Følstad, H. Halpin, P. Kolozaridi, L. Yuldashev, A. Smoliarova, & H. Niedermayer (Eds.), *Internet Science: INSCI 2018 International Workshops, St. Petersburg, Russia,*

October 24–26, 2018: revised selected papers (pp. 203-211). (Lecture Notes in Computer Science; Vol. 11551). Springer

Quintais, J. P., Bodó, B., Giannopoulou, A., & Ferrari, V. (2019). Blockchain and the Law: A Critical Evaluation. *Stanford Journal of Blockchain Law & Policy*, *2*(1), 86-112.

CHAPTER 2: PERFECT ENFORCEMENT, PERFECT TARGETING: SPECTERS OF SURVEILLANCE IN THE GOVERNANCE OF FINANCIAL DATA.

2.1 INTRODUCTION

Data regarding financial transactions are a crucial source of information for law enforcement. Financial transactions' data can signal illicit activities such as tax evasion, money laundering, and terrorist financing. Triangulated with other personal data points, they allow an inference of information about individuals' activities, purchases, and geographical movements, from which, in turn, sexual orientation, health status, religious and political beliefs, and cultural preferences can be derived.

Events such as the 2008 financial crisis, 9/11 and the following spread of terrorist activities in the West have incited U.S. and European institutions to enhance the transparency and public oversight of financial intermediaries. Regulatory updates in the European legal frameworks have strengthened the requirements for customer identification, recordkeeping, and data retention for activities involving the transfer and storage of funds. Legal measures have also been taken to prevent wealth from bypassing national fiscal policies by flowing into offshore financial centers. Bank secrecy has been undermined, even in previously established fiscal havens.

The concrete implementation of these policy goals depends, ultimately, on the capillarity of public-private informational networks, which vary among geographical areas and business types.

In the same period of time, another legal priority – also aimed at increasing the trustworthiness of powerful intermediaries – has been pursued by European regulators: privacy. The adoption of the General Data Protection Regulation (GDPR)[24] enhances efforts in granting individuals specific legal rights regarding their own personal data, to be guaranteed by any kind of commercial entity that collects such data for its business purposes.

On the one hand, European regulatory updates on Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) policies and tax administration law demand financial institutions to extensively collect and store personal data. Moreover, the Payment Service Directive 2 (PSD2)[25] obliges financial institutions to share data with Third Party Providers to facilitate the functioning and competitiveness of European payment markets. On the other hand, the GDPR imposes on information intermediaries the principle of data minimization and grants individuals the right to have their data rectified, erased, or transferred according to their will. Financial institutions, therefore, are expected to enforce legal requirements and policy goals that are difficult to incorporate within the same technological and governance structure.

As the modality of the practical, mutual integration of these coexisting legal frameworks is not clearly spelled out by the legal frameworks themselves, their concrete co-applicability is often shaped by financial intermediaries' industry. Automated tools for data processing and bulk collection of personal data are incentivized by law enforcement legal requirements. Moved by efficiency and risk considerations, industry actors minimize their legal liabilities by automating their compliance procedures through technical means of data collection, analysis and elaboration (Frasher & Agnew, 2014). At the same time as private financial intermediaries are moved by commercial incentives, data are involved in channels of commercial exploitation. The resulting technological standards and data practices are oftentimes debatable

---

24 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

25 Directive (EU) 2015/2366 of the European Parliament and of the Council of November 25, 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

from a privacy point of view, so that it becomes fundamental to scrutinize which actors, and which interests, determine the governance of financial informational networks.

This chapter illustrates emerging privacy and data protection issues that derive from the digitalization of the financial infrastructure. The view underlying this study is that the coexistence of privacy and law enforcement legitimates interests required to admit spaces where one goal is sacrificed for the benefit of the other. Physical cash traditionally circumscribes one of these spaces, as it allows untraceable transactions preserving privacy at the expense of enforcement capabilities. The digitalization of payment infrastructures and the gradual disappearance of cash, however, is leading to a situation of perfect enforcement: even when the transactions are small-scale, the financial digital architecture does not admit "weak spots" where transactions are not associated with individuals and interlinked with other pieces of information.

Recognizing both privacy and prevention/investigation of illegal activities as legitimate policy goals, this study suggests that regulators should seek institutional arrangements that, while not giving up public interest and security objectives, safeguard financial data from the plurality of surveillance networks expanding in this area. This implies favoring *imperfect* over *perfect* enforcement – conceding, by remotion, legitimate spaces for privacy in financial transactions.

Section 2.2 defines the problem by: (1) circumscribing the concept of "financial data"; (2) illustrating the role of such data in law enforcement and public administration processes; and (3) exposing the data protection normative framework that applies to the processing of financial data. Hence, privacy issues in the financial domain are further scrutinized in light of the most recent industry developments (2.3). Finally, Section 2.4 presents some concluding normative considerations: legal or technical means to enhance privacy and data protection in financial information networks, and techno-institutional arrangements for privacy-enhancing digital payment.

2.2 FINANCIAL DATA BETWEEN LAW ENFORCEMENT PRIORITIES AND PRIVACY CONSIDERATIONS

2.2.1 DEFINITION OF "FINANCIAL DATA"

Neither legal frameworks regarding data collection and retention for law enforcement purposes, nor privacy legal instruments, identify a notion of "financial data". The present chapter, consistent with this approach, refers to "financial data" without suggesting the existence of a *sui generis* kind of data generated in the context of financial activities. Rather, the term "financial data" is used, for the purpose of this chapter, to refer to data that (a) is linked to an individual or more individuals (data subject), and that is either (b) (i) directly tied to a financial account, transaction or customer's credit profile (data type), or (ii) involved in a financial process (data use) (Lux & Shackelford, 2020). This definition is practical as it allows the scope of the study to be narrowed without relying on the identification of the legal entity involved in the transaction, and without differentiating between personal data based on the use (commercial or law enforcement) that is made of it.

Different kinds of personal data are involved in financial activities. Data that is strictly related to financial transactions can be referred to as *transactional data*, i.e., the amount of funds transferred from x to y. The PSD2 identifies the category of *sensitive payment data*, defined as "data, including personalized security credentials which can be used to carry out fraud"[26] – e.g., credit card numbers and security codes. However, financial intermediation implies the transmission, storage, and elaboration of a wide variety of personal information that goes well beyond the mere recording of transactions' values and accounts' identifiers. Personal data is collected (and acquired from third party service providers) and used by financial firms for multiple reasons, which can broadly be categorized as: (a) performance of the service, as specified by the contract between the service provider and the customer; (b) user profiling for marketing purposes; or (c) legal compliance obligations.

The aggregation and analysis of transactional data with other personal identifiable information and the prolonged observation of patterns in financial

26 Article 4(32) PSD2.

activities serve the creation of datasets, which we can define as *derivative* data. This category of triangulated, elaborated data often constitutes the information that financial intermediaries hand over to law enforcement agencies and to various third parties to build customer profiles for credit risk analysis. The sub-derivative data that constitute profiling are furthermore involved in automated decision-making processes, and building intelligence and marketing strategies.

2.2.2 FINANCIAL DATA AND LAW ENFORCEMENT

The traditional study of politics by Harold Lasswell (1936) locates information among the resources that are key to the art of *statecraft*. The government of modern societies is organized around knowledge. Sovereign states need data about citizens to administer the wealth and behaviors of large populations (Foucault, 1991). The collection, sorting, organization, and analysis of massive amounts of data are fundamental to large-scale political economies. Data-based administration is thus the prominent form in which (political, social, and economic) power manifests itself, and is exercised in modern society.

Financial records are particularly crucial for law enforcement processes. The administration of welfare policies largely depends on governments' ability to access financial databases and records of both individuals and businesses transactions.[27] Abolishing anonymity is the primary step to eradicating welfare fraud and detecting criminal undertakings. Centralized firms and institutions are entrusted to gather, access, and manipulate the information that is necessary to protect the security and correct functioning of the financial system. Forms of *information mercantilism* (Rosenbach & Mansted, 2019) have long tied together law enforcement apparatuses and financial firms. Managing wealth in the form of credit and debt recording, financial intermediaries operate in liaison with administrative agencies and cover roles that some political economists have targeted as quasi-public (Litan et al., 2002; Selmier & Frasher, 2012). Financial information agents, therefore, are responsible not only for the economic stability of a monetary system, but also for the trustworthiness of administrative and judicial processes.

---

27 See also: Porter T.M, 2020; Scott J.C., 1998; Lauer J., 2017.

Demands for greater transparency, better recordkeeping and oversight of financial information channels have increased steeply in the aftermath of the 2008 financial crisis (Campbell-Verduyn et al., 2019). In the EU, legislative frameworks have been updated to enhance the pressure on financial institutions to share data with other financial institutions, government agencies, and international bodies.[28] The 5th Anti-Money Laundering Directive (5thAMLD)[29] and other legal instruments[30] mandate that financial intermediaries have in place automated systems for customer identification, transaction monitoring and reporting. These compliance processes imply massive data collection, long data retention periods, and the use of automated tools for the detection and red flagging of suspicious transactions.

The digitalization of monetary flows allows the organization of capillary systems of financial surveillance that exceed previously conceivable levels of efficiency. Following the logics of actuarial justice and risk-based regulation, individuals and groups are subjected to automated profiling and decision-making (Hildebrandt, 2009). An extensive legal doctrine discusses the normative issues associated with data-driven, automated decision-making (Yeung, 2018; Pere & Elkin-Koren, 2015; Pasquale, 2015). These issues not only concern privacy and individual autonomy, but also the erosion of the principles of due process, fairness, and equality. Thus, it becomes necessary to define clear boundaries within which efficiency gains can be advanced at the expense of privacy and fundamental rights.

Surveillance-based enforcement networks built around financial databases must be scrutinized both for their dimension and pervasiveness, and for the interests that are involved in their construction and maintenance. The extensive reliance on private intermediaries raises the question of whether these parties are worthy of the trust that enforcement duties imply (Bodó, 2019). As events in 2008 demonstrated, the self-interest of private parties

---

28 For an overview of the actions undertaken in the context of European financial reform, visit: <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-reforms-and-their-progress/progress-financial-reforms_en> last accessed October 15, 2020.

29 Directive (EU) 2018/843 of the European Parliament and of the Council of May 30, 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

30 For example, Directive (EU) 2015/2366, Directive 2006/24/EC.

is not always aligned with public interest. The over-reliance on financial firms to maintain the edifice of risk management determined a collapse of the system. Similarly, entrusting financial corporations with the task of balancing the safety and the privacy of citizens might lead to disappointing outcomes.

Financial entities are not immune to the economic incentives that inform data practices in other industries. Ubiquitous data gathering, required for capillary enforcement, feeds into the logic of accumulation typical of *surveillance capitalism* (Zuboff, 2019). Data becomes a new asset and firms acquire economic power by "channeling and controlling flows of personal information" (Yeung, 2017, p.20). The other face of financial surveillance is, in other words, the emergence of business models that exploit personal information in ways that are often opaque to both individuals and public authorities.[31]

2.2.3. FINANCIAL DATA AND DATA PROTECTION NORMATIVE FRAMEWORKS: A DOUBLE STANDARD?

Financial information is processed and stored by private financial intermediaries in the pursuit of, primarily, commercial interests. The GDPR applies when personal data is processed by commercial entities established within the European Union, or when such data refers to subjects located in the EU.[32] In relation to such processing, the regulation establishes rules and principles aimed at protecting individuals against unfair uses of their personal information. It spells out clear responsibilities for what are termed *data controllers*[33] and *data processors*[34], including obligations to grant individuals a series of rights regarding personal data related to them.

Financial firms' data processing practices are, however, also deeply connected to administration and law enforcement mechanisms. Hence, the data they manage has a dual use and sits in a gray area of data protection. When the legal basis for data processing is the performance of law enforcement-related

---

31 This phenomenon will be explained in Chapter 4 as the *platformization* of the digital payment market.

32 Article 3 GDPR.

33 Article 24 GDPR.

34 Article 28 GDPR.

operations, in fact, the standard GDPR regime gives way to other provisions aimed at balancing data protection legal safeguards with the needs of law enforcement agencies.

The GDPR provision that opens the possibility for law enforcement-related derogations is Article 23. This article provides that EU or national law may restrict the scope of the obligations and rights established by the Regulation for reasons of public security, for the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal penalties, and to pursue "other important objectives of general public interest" including "monetary, budgetary and taxation matters, public health and social security".[35] The conditions for such restrictions to be admissible within the GDPR framework are that they are provided by law, do not interfere with fundamental rights, and are necessary and proportionate in a democratic society.[36]

Indeed, in multiple cases, financial information is used for the purposes listed in Article 23. This is foreseen by Recital 112, which specifies that "derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities".

When law enforcement duties allow private entities to derogate from their GDPR obligations, however, data processing does not take place in a legal vacuum: the regime governing data processing for non-commercial purposes must be found elsewhere. The so-called Law Enforcement Directive (LED)[37] has been adopted to cover what the GDPR had left out: the protection of data that are processed for law enforcement purposes. It applies to: a) public authorities processing data for the purposes of preventing, investigating, detecting or prosecuting of criminal offences, or for safeguarding public

35 Article 23(1) GDPR.

36 ibid.

37 Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89.

security; and b) any other entity entrusted by national law to process data for the above-mentioned law enforcement objectives.[38] Seeking to establish a level playing field across the EU on law enforcement cooperation and related data protection standards, the legal instrument demands national policymakers define the appropriate rules to achieve the stated goals.

Notwithstanding the proposition of GDPR-inspired principles, the LED demonstrates the difficulty of balancing privacy with law enforcement priorities. On the one hand, it values the idea of individual controllership and transparency. On the other, it foresees law enforcement as the only legal basis for processing, excluding by default the need – or even the possibility – of consent (Leiser, 2019).

While the legal instrument lists a number of data subject rights (information, data access, rectification, and erasure rights) it also leaves wide possibilities for national provisions to limit them. Indeed, it is hard to imagine how – for instance, in the context of criminal investigations – data subjects could exercise their rights without compromising the effectiveness of law enforcement activities. Therefore, the possible obstruction of law enforcement processes is foreseen as a justification for denying information or access rights. Similarly, data rectification or erasure claims can be dismissed if the concerned data serves as judicial evidence.[39] As it concerns financial data, such an eventuality presents itself in the context of AML procedures. According to the 5th AMLD, Member States can impose up to seven years of data retention for AML purposes, even after a customer's account has been closed.[40] This will eventually override data subjects' right of erasure.

In short, it can be said that different legal regimes apply when data is processed for commercial purposes or for law enforcement ones. This double standard becomes problematic when law enforcement data processing is performed by private firms, as is often the case with financial data. In fact, data that is collected for economic purposes could then be exploited in the context of legal inquiries or used as evidence. It can be impractical to deter-

38 Article 3(7) LED.

39 Article 16(3)(b) LED.

40 Deloitte, 2018.

mine when one regime should give way to the other, and data subjects can see the GDPR legal protections decrease or vanish when a law enforcement procedure involving their data is initiated.

The resulting situation is one of legal uncertainty that threatens to undermine the principle of purpose limitation. This has been underlined by Article 29 of the Data Protection Working Party (WP29), in its 'Opinion 03/20 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data'. In the document, the WP29 underlines that "the growing number of situations in which activities of the private sector and of the law enforcement sector interact with each other"[41] means restricting exceptions to the right to privacy to the strictly necessary. In making such a statement, the WP29 refers specifically to financial data transfers to law enforcement authorities, and criticizes the failure of the proposed legal instruments "to address the legal uncertainty for situations in which data collected for commercial purposes are used for law enforcement purposes".[42]

Sectorial rules such as those implementing the 5thAMLD, the Market in Financial Instruments Directive framework and the PSD2 can impose data collection and sharing practices that clash with GDPR rules and principles.[43] The complex interaction between the coexisting data protection and data-sharing legal frameworks is not straightforwardly derivable from the combined reading of the legal provisions. It remains the task of national policymakers to define to what extent data protection rules can be derogated from to enable law enforcement processes. And in practice, the way in which the normative goals are balanced between each other determines – and also depends on – the technical design of the data processing tools chosen by the industry (Frasher & Agnew, 2014).

---

41 See also: Article 29 Data Protection Working Party (WP29), "Opinion On Some Key Issues Of The Law Enforcement Directive" <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178> last accessed June 10, 2020.

42 WP29, Opinion 03/2015.

43 See: The Dutch Banking Association, 2019: the report stresses that "financial market participants need further legal clarity around the interactions between AML and personal data legislation".

The 5th AMLD hints at the role of the Financial Action Task Force (FAFT) in delivering international standards for AML compliance.[44] However, while regulatory frameworks and supranational bodies might give guidance, data-transfer protocols and AML software are mostly developed at a firm or industry level. As it concerns interbank and international data-sharing, a central role is covered by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which acts as a world leader in the provision of internationally standardized financial messaging services. The cooperative private entity does not only provide software but also acts as Registration Authority for digital identifiers, such as the ISO 9362 Business Identifier Code (BIC), the ISO 13616 International Bank Account Number (IBAN), and ISO 10383 Market Identifier Code (MIC).

The growing availability of financial data, and the multiplicity of actors that participate in and inform its data processing and exchange processes, demand the scrutiny of financial information networks in light of the European data protection legal frameworks. The next section will expose current trends of the financial industry that are making this task more problematic, threatening to make the financial industry a weak spot in EU privacy protection.

2.3 FINANCIAL INFORMATION NETWORKS: WEAK SPOT IN EUROPEAN PRIVACY PROTECTION?

2.3.1 THE FINANCIAL INDUSTRY (CHANGING) LANDSCAPE: DIGITALIZATION AND DATA ECONOMY

Allowing more or less oversight of information by interested actors, the technological infrastructures and the concrete operations in which personal data is involved determine the degree to which privacy policies are enforced. Our analysis seeks to picture how the compromise between privacy and law enforcement is framed in practice. Understanding this practice requires assessing who the information agents involved in data exchanges are; what kind of information they gather, and for which purposes; which roles these agents perform; under which terms and legal obligations they collect, use and share information; and with which other actors they share such information.

---

44 Recital 4 AMLD.

In the past decades, two major tendencies have emerged that urge to bring the issue of financial privacy into the spotlight. The first one is the increased digitization of money and commerce, which has exponentially expanded the production and availability of financial data. In 2019, countries like Sweden and the Netherlands recorded a higher total amount of digital transactions than cash-based ones, showing a tendency toward substituting cash even for small payments (Van Paassen, 2020). This trend is interrelated with a wave of "technology-enabled innovation in financial services" that results in "new business models, applications, processes or products with an associated material effect on the provision of financial services".[45]

The second tendency is the reconfiguration of the incentives underlying the provision of financial services around data exploitation.[46] New tools for data collection and processing, and possibilities of intersecting financial data with additional information about users' online activities, situate financial information networks within the logics of the contemporary information economy. Arguably, technology has changed practices and modalities of money circulation, and therefore it has reshaped our expectations regarding information management. New actors such as electronic payment providers (PayPal, AliPay) and plastic card issuers (MasterCard, Visa) acquire worldwide dominant positions largely due to the optimization of services that data aggregation allows.

The landscape of financial service providers that intermediate transactions, allocate credit, and store value via electronic networks is composite and dynamic. Banking institutions constitute the backbone of global financial flows. Moreover, ancillary yet heavily influential service industries have developed and expanded in worldwide markets. These are, mainly, credit and debit card providers and, more recently, electronic payment providers

45 Financial Stability Board, "Monitoring of FinTech" (2017). Examples of such innovative applications are various account aggregation tools such as *open banking* and *screen scraping*, or robo-advice services; see: OECD, 'Personal Data Use in Financial Services and the Role of Financial Education: A Consumer Centric Analysis' (2020) www.oecd.org/daf/fin/financial-education/Personal-Data-Use-in-Financial-Services-andthe-Role-of-Financial-Education.pdf> last accessed October 14, 2020.

46 European Banking Federation, 'Data usage, access & sharing in the digital economy' (2020) <https://www.ebf.eu/wp-content/uploads/2020/02/Data-economy-EBF-position-paper-Jan-2020.pdf> last accessed June 10, 2002; World Economic Forum, 'The Appropriate Use of Customer Data in Financial Services' (2018) <http://www3.weforum.org/docs/WP_Roadmap_Appropriate_Use_Customer_Data.pdf> last accessed June 10, 2002.

(e.g., PayPal, AliPay). Finally, a wide variety of non-financial actors process financial data in the context of their commercial activities: retail sellers in physical shops, online e-commerce platforms, credit reporting agencies, insurance companies, marketing agencies, etc.

It is beyond the scope of this chapter to focus on specific financial intermediaries or to define the differences in their functions and data practices. Instead, I want to offer a picture of what the ongoing transition from physical to digital means of payment implies in terms of privacy. Along with electronic payment, mobile banking businesses are examples of "FinTechs that challenge the traditional financial service sector", as they successfully provide services which "adjust retail banking to the modern, mobile lifestyle of today's customers".[47] The terms mobile banking, mobile payments, and mobile transfers refer to various kinds of applications developed to enable storage and transfer of money electronically, via mobile devices such as smartphones and tablets. These types of applications can be developed by existing banking institutions or provided by firms – such as bunq, Revolut and N26 – that center their business models and products solely around mobile services. As these entities are modeled according to the logics of the data economy, their practices in terms of personal data are considered in the next sections to discuss privacy issues deriving from the latest technological developments of the financial industry.

2.3.2 PRIVACY LOOPHOLES IN FINANCIAL INTERMEDIARIES' DATA PRACTICES

2.3.2.1 THE DUAL USE OF FINANCIAL DATA

The processing of personal data for commercial purposes falls under the scope of application of the GDPR, which limits such processing in order to protect the fundamental rights of data subjects. However, Article 23 of the GDPR establishes that overriding legal obligations can justify restrictions of such rights. The rights to data portability[48] and data erasure[49], for exa ple, are

47 Private Equity Forum, 'Brief insights from PEF research. N26: the rise of a fintech' (2018) <https://pef-jlu.de/wp-content/uploads/2018/10/heyden_poppelreuter_2018_brief_insights_n26.pdf> last accessed June 10, 2020.

48 Article 20 GDPR.

49 Article 17 GDPR.

not granted with regard to data collected in the context of AML procedures. Other examples are Member States' national laws establishing commercial and tax retention periods. For instance, under the German Commercial Code (Handelsgesetzbuch), Tax Code (Abgabenordnung), Banking Act (Kreditwesengesetz), Money-laundering Act (Geldwäschegesetz), and Security Trading Act (Wertpapierhandelsgesetz), the German mobile bank N26 must retain customers' data for a period of two to ten years.[50]

Limitations to the applicability of privacy rules are relevant in light of the recent development of the financial service industry toward ever more data-intensive business models. New mobile banking service providers raise particular concerns about the practices of data collection and surveillance that they facilitate.[51] For example, Revolut's privacy statement reveals that the company exploits a wide variety of information for marketing purposes, including the personal information provided by a user to initiate the service, information acquired from social media platforms ("if you allow us to, we will collect information such as friends lists from Facebook or similar information from other online accounts"), information from the user's' device ("contact information from your address book, log-in information, photos, videos or other digital content, check-ins") and information about the user's location. Such personal data is shared by default with credit agencies, social media companies, and analytics firms. [52]

The German mobile banking service provider N26 announces in its privacy policy its use of "Social Plugins": by clicking on Facebook, Twitter, LinkedIn, or Instagram plugin buttons, users establish a connection between N26's application and the social media's servers. The social media platform receives information about the user's visit on the banking app. Regarding this data transmission, N26's privacy policy remains vague, merely stating that "as provider of the pages, we do not receive any information on the contents of the data transmitted and their use by Facebook/Twitter/LinkedIn/Instagram"[53].

---

50 N26 Privacy Policy https://docs.n26.com/legal/06+EU/03+Privacy%20Policy/en/01privacy-policy-en.pdf.

51 See: Martin, 2019.

52 Revolut Privacy Policy. https://www.revolut.com/legal/privacy.

53 N26 (n 42).

Moreover, data is shared with third parties in order "to display specific ads to our customers or to exclude them from specific campaigns". In particular, using Facebook, Google, and Zeotap Custom Audience services, the bank transmits users' email addresses to social media platforms in order to enable the matching of users' profiles with the data possessed by such third parties. No clarification is given about the use that these third parties will make of the shared data.

In theory, the principle of purpose limitation prohibits data collected for law enforcement purposes being used for commercial ones, and vice versa. However, in the case of financial intermediaries, reasons of legal compliance and private commercial interests can overlap.

Granular and systemic collection of personal data, in fact, is mandated by sectorial regulation (e.g., MiFID II, 5th AMLD, Transparency Directive, PSD2, national fiscal laws) aimed at ensuring that transparency, risk management, and fraud detection processes are in place. This triggers the exceptional regime allowed by Article 23 of the GDPR. However, such efficiency and risk management goals are part of normatively protected public interests, as well as of a firm's economic strategy. It is historically accepted that financial intermediaries are custodians of sensitive information: this allows them to support both administrative/judicial processes on one side, and citizens' interaction with the larger economic system on the other. Such a position, however, becomes critical when financial entities expand their data extraction processes to non-financial aspects of private life, intersecting economic information with data points collected by social media or users' devices. Financial firms' data collection strategies should, therefore, be scrutinized by considering both the economic interests that incentivize them, and the important decision-making processes they inform (regarding taxation, insurance, credit allocation, and judicial investigations).

Finally, the purpose limitation principle is hard to implement because of the fluid nature of enforcement processes. In fact, data previously collected for commercial purposes can then become useful in the context of criminal investigations or required for intelligence operations. In such cases, users can have their privacy legal protections diminished without being informed about it.

2.3.2.2 FOREIGN ACCESS TO FINANCIAL DATA

An interrelated aspect that affects the enforcement of European privacy policies is the cross-national nature of financial services, and of the law enforcement networks that are tied to the related data flows. Regulating cross-border data-flows is particularly tricky where financial data are concerned. On the one hand, while they expand their businesses across jurisdictions, financial service providers have an interest in managing global customers data in a centralized manner (Selmier & Frasher, 2012). On the other hand, the governance of their databases is affected by multiple national legal frameworks, as they cover important roles as information agents for national and international law enforcement agencies.

Financial intermediaries move data across countries for a variety of reasons. Often, transaction data is cross-border by nature. Moreover, gathering information in centralized places enables better analytics for risk management, and the tailoring of products at regional and local levels.[54] Such movement of data across borders is not, however, uncontroversial from a law enforcement and data protection point of view. In fact, data protection rules established for firms and public authorities in the EU do not always have equivalents in other jurisdictions.

Differences between the EU and the U.S. privacy traditions have, in the past few decades, raised controversies about data-sharing practices between law enforcement authorities and financial institutions in the two jurisdictions. Critical differences pertain, for instance, to data retention periods (up to 80 years for U.S. companies, not more than 7 years under the 5th AMLD)[55] and limitations on the commercial use of data (in the EU, firms are bound by the principle of purpose limitation, while in the U.S. the commercial use of data collected for enforcement purposes is not prohibited). Under the Bank Secrecy Act,[56] and the Patriot Act,[57] the U.S. government enjoys

54 ibid.

55 Recital 21 AMLD.

56 The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 U.S.C. 5311 et seq.).

57 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act).

wide-ranging powers to obtain data from financial intermediaries, and the latter are unlikely to deny requests of data access from federal authorities.

This is a matter of concern, as what happens with U.S.-based financial firms has ramifications all over the world. The impact of these differences in terms of privacy, surveillance, and geopolitical power imbalances becomes glaring if one considers the global pervasiveness of the U.S. financial service industry. While traditional banking is still mainly dominated by local actors, the credit and debit card industry is monopolized by U.S.-based companies (Mastercard[58] and Visa[59]) that make transaction data available to U.S. government and enforcement agencies (e.g., under the Patriot Act). The same can be said about the remittances industry (Western Union, Moneygram, and Euronet) and, importantly, the electronic payment service industry (with PayPal in the front line).[60]

Since banks and other financial services conduct business in many nations but their servers store information from clients around the globe, the location of the server can mean that a European citizen's personal data housed or backed up in New York could be ripe for a subpoena from the U.S. government (Frasher & Agnew, 2014, p.8).

The reach of the U.S. intelligence over European financial data became a matter of concern when, in 2006, the *New York Times* revealed the Treasury's Terrorist Finance Tracking Program (TFTP), secretly approved by the Bush Administration to pull EU citizens' data from SWIFT. It was disclosed that the U.S. had secretly subpoenaed the Belgian company SWIFT to hand over

---

58 Mastercard's 'Global Privacy Notice' states that the company shares customers' personal information with Mastercard's headquarters in the U.S and with "other countries which may not have the same data protection laws as the country in which [the user] initially provided the information". https://www.mastercard.us/en-us/vision/corp-responsibility/commitment-to-privacy/privacy.html#dataTransfer.

59 Visa's Global Privacy Notice states that: "Visa is based in the United States and has Affiliates and service providers around the world. Your personal information may be transferred to other countries, which may not have similar privacy or data protection laws." https://www.visa.co.uk/legal/global-privacy-notice.html.

60 PayPal's User Corporate rules state, at the time of writing, that "Most User Personal Data is collected and stored in the United States. PayPal's global business requires User Personal Data to be shared with other PayPal entities in the United States and globally where PayPal currently has or intends to have a presence." https://www.paypalobjects.com/marketing/ua/pdf/GB/en/bcr.pdf (last accessed: November 2022).

information about individuals suspected to be tied to the 9/11 attack. As the servers of the worldwide financial telecommunication network were located in the U.S., the company handed the personal data of EU citizens to U.S. authorities without applying the legal protections established by EU law.

After the controversy, the company moved its servers to the EU, and – notwithstanding initial pullbacks by the European Parliament[61] – a new agreement between EU and U.S. authorities was concluded in 2010 (SWIFT II).[62] Today, however, concerns about the SWIFT Agreement still exist. Edward Snowden's revelations demonstrated that "the US National Security Agency (NSA) has had direct access to the IT systems of a number of private companies and gained direct access to financial payment messages referring to financial transfers and related data"[63] covered by the agreement. In 2013, based on alleged violations of data protection principles of purpose limitation, necessity and proportionality, the European Parliament voted for a suspension of the Agreement,[64] but the Commission has failed to follow up on this decision.

2.3.2.3 PROFILING AND AUTOMATED DECISION-MAKING

The high volume of data processing performed by financial intermediaries involves the deployment of automated or semi-automated systems for data collection and analysis and algorithm-based consumer profiling.[65] N26, for example, uses semi-automated data processing "to assess certain personal aspects (profiling)" for the purposes of AML and crime prevention, targeted marketing, and credit risk scoring. Such automated evaluation mechanisms involve the elaboration and matching of a wide variety of personal data

61 Toby Vogel, 'EU, US sign SWIFT agreement - MEPs' demands for changes accepted', (*Politico*, June 28, 2010) <https://www.politico.eu/article/eu-us-sign-swift-agreement/. For an overview of the controversy about the SWIFT agreement and the TFTP, see: Cristina Blasi Casagran, *Global data protection in the field of law enforcement: An EU perspective* (Routledge 2016).

62 Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.

63 European Parliament resolution of October 23, 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)).

64 ibid.

65 OECD (n 38)

including salary, expenses, existing obligations, job, duration of employment, experiences with former contractual relations and credit solvency, "as well as credit agencies' information".[66]

The 5th AMLD does not refer to the use of automated or semi-automated mechanisms. However, it mandates "consumer due diligence", which comprises "ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship".[67] Moreover, obliged firms must send Suspicious Transactions Reporting (STR) to competent Financial Intelligence Units (FIUs). As acknowledged by Europol in its 2017 report on European financial intelligence:

> The increasing digitalisation of financial services results in growing volumes of transactions and extremely large data sets requiring computational analysis to reveal patterns, trends, and associations. The use of analytics is therefore becoming essential for both reporting entities and FIUs to cope with information and fully exploit its potential.[68]

Customer due diligence and STR are performed through software – made available by technology companies – that uses machine learning for the automated processing of data for customer profiling, transaction monitoring, and red flagging. Their output can trigger – based on behavioral patterns and data association – a criminal investigation or denial of a financial product.[69]

Profiling[70] and automated decision-making[71] in the context of AML procedures are legitimate under Article 6(1c) of the GDPR, which establishes a legal basis for automated data processing that is "necessary for compliance with a legal obligation". Article 22 of the GDPR sets out a general prohibition for a

66 N26 (n 42).

67 Article 13, AMLD.

68 Financial Intelligence Group (2017).

69 See, for instance: Accenture Consulting, 'Evolving AML journey - Operational transformation of anti-money laundering through robotic process automation'. https://www.accenture.com/_acnmedia/PDF-61/Accenture-Operational-Transformation-Anti-Money-Laundering-Robotic-Process-Automation.pdf.

70 Defined by Art 4(4), GDPR.

71 Making decisions by technological means without human involvement.

"solely automated individual decision", including profiling, which might have a "legal effect" or be "significantly affecting" for the data subject. However, a decision based solely on automated processing, including profiling, can be allowed when it is: (i) necessary for entering or performing a contract; (ii) authorized by law; or (iii) based on consent.[72] Recital 71 specifies that decision-making based on automated processing, including profiling, shall be allowed when foreseen by national law for fraud and tax-evasion monitoring and prevention purposes, and "to ensure the security and reliability of a service provided by the controller".

The WP29 has underlined how profiling and automated decision-making, even when deployed in the context of law enforcement activities, must respect data protection principles and be grounded on a legal basis specified by national law.[73] A data subject should be granted the right to obtain human intervention from the controller and to "express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision".[74] It is questionable, however, whether such rights are granted in the context of automated AML procedures carried out by financial firms. In fact, customers are not informed when reporting is made to FIUs or when a profile has been red-flagged. Moreover, algorithm-based transaction monitoring and law enforcement can lead to unfair implementation of compliance procedures. Red flagging and investigation procedures can be triggered by biased automated mechanisms, based on systematic discrimination and stereotyping mechanisms.

Automated data processing and profiling are heavily deployed for credit rating and personalized marketing based on consent. In the opinion of WP29, however, profiling and automated decision-making can involve opaque processes, based on data "that is derived or inferred from other data, rather than data directly provided by the data subject".[75] Hence, if these practices are justified based on consent, data controllers must ensure that data

72 Art. 22(2)(a)(b)(c), GDPR.

73 WP29, 'Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679'.

74 Recital 38, LED; Article 22, GDPR.

75 WP29 (n 66).

subjects are properly informed about the consequences of data processing, and safeguards must be in place to ensure "fairness, non-discrimination and accuracy in the profiling process".[76]

Recital 47 concedes that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest". However, the WP29 reiterates its precedent opinion that "it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering".[77] Moreover, the standards for meeting the legitimate interest requirement should be higher when considering the comprehensiveness of the profile and the relevant impact of such profiling. Credit reporting and scoring, in fact, can significantly impact life opportunities of individuals, determining their likelihood of receiving loans or being offered one rather than another financial product.

On the impact of automated surveillance systems on privacy and liberties, a landmark decision has recently been issued by the Court of The Hague. In the ruling, the Dutch SyRI Act – regulating the use of the Systeem Risico Indicatie, an automated system for detecting various kinds of welfare fraud – has been found in violation of Art. 8 of the European Convention on Human Rights. The ruling sets an important precedent in limiting the use of predictive and automated detection systems for law enforcement that contravene fundamental human rights. The Court stressed that Member States must strike "the right balance between the benefits associated with the use of those technologies on the one hand and the interference that can make use of the right to respect for private life on the other".[78]

---

76 ibid.

77 WP29 (n 85) recalling WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Art 7 of Directive 95/46/EC (2014).

78 *NJCM et al. and FNV v The State Of The Netherlands* [2020], ECLI:NL:RBDHA:2020:865.

2.4 CONCLUSIONS

This chapter illustrates how, in the governance and regulation of financial data, privacy considerations are compromised through law enforcement priorities. Access to citizens' financial status and activities are deemed necessary for taxation purposes, welfare administration, and crime prevention. Tracking financial records facilitates the efficient allocation of resources, and the administration of welfare and criminal policies. As these motivations inform the management of financial data, the operability of GDPR legal protections is partially compromised.

The GDPR, in fact, allows exceptions to privacy protection when law enforcement legal obligations are imposed – e.g., by AML legal rules – on information intermediaries. However, the wordings of the LED, the GDPR, and the 5th AMLD, as well as the opinion expressed by WP29, indicate that law enforcement policies must respect the principles of data protection (i.e., data minimization, and purpose limitation) and be limited to what is strictly necessary, respecting fundamental individual rights.

Compromising privacy in the name of law enforcement is a slippery slope. The reasons justifying data collection and processing by financial institutions are not always univocal: the very same pieces of data and their triangulation can serve multiple purposes. Notwithstanding the semi-public roles that financial intermediaries are ascribed based on their positions as information agents, such entities are commercial players incentivized by profit maximization goals. Data gives financial firms competitive advantage over other financial firms, allowing them to target products and services at territorial and individual levels. This data is also exchanged with third parties for credit risk profiling. Processed in automated ways for individual profiling, marketing, algorithmic predictions and re-engineering of behaviors, financial data enter the logic of accumulation typical of the data economy.

Exposing financial intermediaries' practices of data exploitation, and issues related to the transfer of those data to third parties – including foreign law enforcement agencies and social media platforms – this chapter argues that financial data constitutes a weak spot of European privacy protection. The analysis provided here suggests that legal clarification is necessary:

a) regarding the implementation of the purpose limitation principle, to ensure that financial data collected for law enforcement purposes is not abused in commercial data-intensive strategies; b) on the jurisdictional limitations of law enforcement data access; and c) on the use of automated decision-making and profiling by financial intermediaries, as part of their compliance processes, credit risk scoring, and marketing strategies.

As physical cash is replaced by digital means of payments even for small transactions, financial data becomes increasingly available, informative, and interlinkable with various pieces of personal information. The capillarity and ubiquity of financial surveillance performed through automated data processing limits individual freedom and autonomy, threatening fairness and indiscrimination in administrative and criminal procedures. Based on the view that the coexistence of privacy and law enforcement goals requires the admission of spaces where one goal is sacrificed for the benefit of the other, I argue that the law should allow and even encourage the construction of tools for digital transactions unlinked from identifiers.

CHAPTER 3: THE LEGAL CATEGORIZATION OF THE OUTSIDE: THE REGULATION OF CRYPTO-ASSETS

3.1 INTRODUCTION

Blockchain technology, with its fundamental proposition of transparency and cryptographically secured systems of rights' enforcement, has fuelled hyped attention across many areas, spanning from trade to copyright protection. So far, however, the most widespread and disruptive innovation introduced by the technology remains what are termed cryptocurrencies and, more generally, the possibility to create units of value that circulate on a worldwide, peer-to-peer digital network.

Rooted in open-source cultures, the rise of blockchain-based financial networks expresses a neo-libertarian response to the post-2008 crisis of trust in political and financial institutions (Faria, 2019, p. 119). Among the speculations on what this technology could deliver is the belief that it can nurture new, horizontal socio-economic organizations (De Filippi & Wright, 2018), and help increase transparency in institutional processes (Werbach, 2018). The development of the industry, however, shows that the inherent values of decentralization and transparency are increasingly challenged at all layers of the socio-technical blockchain stack (Bodó & Giannopoulou, 2019). Without the appropriate legal safeguards, the *privatisation of money* that blockchain enables could entail the concentration of financial and political power in the hands of a few unaccountable actors (Lehdonvirta & Vidan, 2019).

When new "disruptive" technologies emerge, regulators must identify inherent risks and develop policy strategies to balance the various interests that innovation touches upon. To do so, it is critical to take a step back from techno-solutionism and look beyond the ideological narratives on *decentralized money* as an emancipatory social artifact, to scrutinize how actual entities, economic relationships, and technological solutions develop vis-à-vis existing institutions and market players.

In light of the rapid development of the blockchain industry and of the interest, from European institutions, in promoting the use of the technology for financial applications (fintech), the present chapter provides an overview of the most important legal frameworks that are applicable to blockchain-based financial applications under European law. Exposing shortcomings and drawbacks in the applicability of existing regulation, this chapter seeks to inform the current debate on the need for regulatory intervention at the EU level in this domain.

To provide context for the reader, Section 3.2 introduces the notions of crypto-assets, their use cases and the main legal issues emerging around them. Section 3.3 deals with the legal qualification of crypto-assets under the EU legal framework, describing the typology of tokens accepted by EU financial institutions. Sections 3.4 and 3.5 draw on the guidelines issued by the European Securities and Market Authority (ESMA), and by the European Banking Authority (EBA), respectively, to provide an overview of the legal treatment of tokens that qualify as investment instruments and as electronic money. In this context, legal and enforcement issues raised by blockchain-based financial applications are outlined. The conclusion summarizes the major findings and highlights issues of relevance for policy development and further research.

3.2 CRYPTO-ASSETS: DEFINITION, USE CASES AND LEGAL ISSUES

Blockchain-based tokens can be described as digitally scarce units of value, the properties and circulation of which are prescribed via computer code. As their possible uses are potentially unlimited, the present chapter will use the term *crypto-asset* to encompass the wide variety of virtual currencies, virtual assets, and digital tokens that blockchain can support.

The first cryptocurrency, Bitcoin, was created to function as a means of payment, but it quickly turned into a store of value subject to speculative interests. Later experiments such as the Ethereum project expanded the functionalities and diffusion of crypto-assets, building upon smart-contract solutions, easing the ability to create and circulate digital tokens on demand.

In mid-2018, the *token economy* reached significant weight in terms of market capitalization.[79] Tokens were created and distributed by firms and platforms with a variety of purposes. Primarily, they can grant users access/participation to online services; they can serve as a means of payment or assure the right to purchase products; or they can represent a stake in the issuer's company, eventually conveying ancillary rights such as voting within the platform's governance system (Adhami, Giudici, Martinazzi, 2017, p.64). Based on these functions, crypto-assets are commonly placed under three main categories, namely utility, payment, and investment tokens (see below for a description of such categories), each of which implies specific legal consequences.

Since 2017, crowdfunding schemes based on Distributed Ledger Technologies (DLTs) – so-called Initial Coin Offerings (ICOs) – have gained worldwide visibility. ICOs consist of the public sale of tokens over online websites and platforms, aimed at collecting funds for the initial development of a project or start-up. Users' participation in ICOs is motivated by the willingness to support a project, and/or by the expectation of future profits deriving from the increase in value of the token. Unless specific limitations are in place, tokens can be traded on cryptocurrency exchanges, with direct access to a voluminous secondary market (Adhami, Giudici, Martinazzi, 2017; Fisch, 2019; Amsden & Schweizer, 2018; Catalini & Gans, 2018).

Because of their purely digital nature and disconnection from traditional financial instruments and venues, ICOs have developed into a regulatory gray area, often outside of the scope of existing legal frameworks. Usually they take place without applying the rules governing the public placement of securities (Adhami, Giudici, Martinazzi, 2017), and without the involvement of traditional financial intermediaries. This allows part of the legal compliance

79 ICO Watch List: https://icowatchlist.com/statistics/year.

costs to be cut[80], which makes this form of crowdfunding suitable for start-ups and innovative businesses – including fraudsters – that could find it difficult, too costly, or unappealing to access traditional funding channels (ESMA, 2019[81]).

European institutions and Member States have started various initiatives exploring blockchain's potential in the financial sector.[82] However, regulators also perceive that blockchain-based financial activities cannot continue to evolve in a legal vacuum, as they raise serious risks related to consumer/investor protection, market integrity, and financial crimes (ESMA, 2019). Regulators and supervisory authorities, therefore, are tackling questions on the legal treatment of crypto-assets and looking for strategies to enforce regulation on the businesses emerging around them.

To understand how to support the development of the industry while ensuring appropriate legal oversight, European as well as National Competent Authorities (NCAs) have opened public consultations and issued extensive reports on crypto-assets.[83] On the one hand, legislators are willing to encourage the *token economy* as a positive "long-term trend", avoiding burdensome regulation that could jeopardize the industry and displace the market for investments. On the other hand, they recognize that legal safeguards and regulatory certainty must be in place, not only to guarantee investor protection, but also to ensure sustainable development of businesses and of the whole ecosystem (ESMA, 2019).

80 However, initiators of ICOs face significant other costs related to technology and token sale system development, and, importantly, marketing. See: G. Zhai, 2018.

81 European Securities and Markets Authority (ESMA), 'Advice on Initial Coin Offerings and Crypto-Assets', ESMA (2019).

82 See, for instance: the Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action Plan. For a more competitive and innovative European financial sector, COM(2018) 0109 final (FinTech Action Plan); European Commission, 'The European Blockchain Partnership', European Commission (2020), https://ec.europa.eu/ digital-single-market/en/blockchain-technologies; The European Blockchain Observatory and Forum, https://www. eublockchainforum.eu; The International Association for Trusted Blockchain Applications, https://inatba.org.

83 For example, Financial Conduct Authority (FCA), 'Guidance on Cryptoassets. Feedback and Final Guidance to CP 19/3, Policy Statement PS19/22 (2019)', FCA (2019), https://www.fca.org.uk/publication/policy/ps19-22.pdf; Assemble´e nationale, 'Rapport d'information en conclusion des travaux d'une mission d'information relative aux monnaies virtuelles', Assemble´e nationale (2019), www.assemblee-nationale.fr/dyn/15/rapports/cion_fin/l15b1624_rapport-information.

Moved by the intention to maintain a precarious balance between liberal positions and legal protections, European institutions have so far adopted a "wait-and-see" approach, refraining from pronouncing on the proper regulatory strategies to be adopted. But in the meantime, some national initiatives threaten to fragment the legal framework across the EU.[84]

EU policymakers are concerned that not only a European, but also an international approach would be necessary to effectively regulate these new financial networks (ESMA, 2019). As crypto-assets' market players operate globally, in fact, regulatory and enforcement efforts at a national level might push firms toward less regulated jurisdictions. This would mean missing market opportunities, as well as jeopardizing investor protection, because tokens can be sold to European investors from other jurisdictions as well. Given this risk of regulatory arbitrage, a balanced regulatory approach is preferable in order to bring crypto-assets and related businesses under the EU jurisdiction and enforcement capacities.

3.3 A (PRECARIOUS) TAXONOMY OF CRYPTO-ASSETS

Key to the definition of the appropriate legal treatment for blockchain-based tokens is the identification of the legal categories under which – based on their specific functions – they can be collocated. As blockchain-based digital assets can be created for different purposes and perform a variety of functions, they can potentially fit multiple legal categories.

In the absence of an agreed-upon, comprehensive taxonomy of crypto-assets, European financial authorities follow a widely accepted classification that distinguishes tokens into three main classes – payment, utility, and investment tokens – based on the different functions that they can perform.

Payment tokens are meant to be used as a means of payment for goods or services external to the platform on which they are issued. In practice, however, the suitability of cryptocurrencies as a means of exchange is often hampered by the high volatility in price (Kharif, 2018; Yermack, 2015), and/or by the "fees" that users must pay for miners that users must pay for miners to

84 Bespoke regulatory regimes have been adopted in Gibraltar, Malta, Liechtenstein, and France.

validate transactions.[85] Even if they typically do not confer further associated rights, cryptocurrencies such as Bitcoin and Litecoin, designed as a means of exchange, can generate profit through price increases, and can be purchased for investment purposes (EBA, 2019)[86].

Investment tokens are considered in some ways equivalent to shares, bonds, or units in collective investment vehicles, as they promise investors future financial benefits, and/or rights in relation to the project they are attached to. Typically, investment tokens are issued – in exchange for dollars, euros, or other crypto-assets – as part of ICOs, in order to raise initial capital for projects. Investors expect financial benefit from the increase in market price of the token/share, but can also be promised a distribution of the future company's profits (similar to the distribution of dividends), and/or voting rights.

Finally, tokens can be issued to grant access to a platform, the use of a service, or the right to purchase a product. These are so-called utility tokens, an example of which is Filecoin. Attached to a decentralized storage network, Filecoin tokens function as a reward for users providing storage space to the network, and can be spent to store and retrieve data thereon (Protocol Labs, 2017).

The flexible design of digital assets implies that they can combine these functions with each other. For instance, tokens that are distributed for utility purposes can entail an investment component as well (Hacker & Thomale, 2018; SEC, 2017). Different functions can coexist in the same token simultaneously, or in different phases of the token's life cycle, adding a temporal dimension to the problem of tokens' legal classification.

---

85 A recent experiment to tackle the issue of price volatility are *stablecoins*, the value of which is asset-backed (in physical collateral or crypto-assets) or algorithmically controlled. However, they are not without controversy, due to their alleged lack of transparency. For instance, there has been claims that the stablecoin Tether is used to manipulate other cryptocurrencies' prices.

86 European Securities and Markets Authority (ESMA), 'Advice on Initial Coin Offerings and Crypto-Assets', ESMA (2019).

3.4 INVESTMENT TOKENS

3.4.1 CRYPTO-ASSETS AS TRANSFERABLE SECURITIES UNDER MIFID II

The qualification of crypto-assets as a *financial instrument* [87] (or more precisely as *transferable securities*) is crucial as it determines the applicability of an extensive set of European and national legal instruments that regulate the EU financial market and the activities/services provided therein. Such rules include the legal frameworks set out by the Markets in Financial Instruments Directive (MiFID II)[88] and the Markets in Financial Instruments Regulation (MiFIR)[89], the prospectus regime established by the Prospectus Regulation[90] and the Prospectus Directive,[291] the Market Abuse Regulation,[92] the Transparency Directive,[93] the Central Securities Depositories Regulation,[94] and other legal instruments that apply to specific activities or types of financial instruments.

---

87 A list of what constitute a *financial instrument* is contained in Directive 2014/65/EU of the European Parliament and of the Council of May 15, 2014 on markets in financial instruments, amending Directive 2002/92/EC and Directive 2011/61/EU, [2014] OJ L 173/349 (Directive 2014/65/EU).

88 Directive 2014/65/EU.

89 Regulation No. 600/2014/EU of the European Parliament and of the Council of May 15, 2014 on markets in financial instruments, amending Regulation (EU) No. 648/2012, [2014] OJ L 173/84 (Regulation N. 600/2014/EU).

90 Regulation No. 2017/1129/EU of the European Parliament and of the Council of June 14, 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, repealing Directive 2003/71/EC, [2017] OJ L 168/12 (Regulation No. 2017/1129/EU).

91 Directive 2003/71/EC of the European Parliament and of the Council of November 4 2003 on the prospectus to be published when securities are offered to the public or admitted to trading, amending Directive 2001/34/EC, [2003] OJ L 345/64 (Directive 2003/71/EC).

92 Regulation No. 596/2014/EU of the European Parliament and of the Council of April 16, 2014 on market abuse (market abuse regulation), repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, [2014] OJ L 173/1 (Regulation No. 596/2014/EU).

93 Regulation No. 596/2014/EU of the European Parliament and of the Council of April 16, 2014 on market abuse (market abuse regulation), repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, [2014] OJ L 173/1 (Regulation No. 596/2014/EU).

94 Regulation No. 909/2014/EU of the European Parliament and of the Council of July 23, 2014 on improving securities settlement in the European Union and on central securities depositories, amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012, [2014] OJ L 257/1 (Regulation No. 909/2014/EU).

The question of whether tokens can fall within the scope of security regulation was addressed for the first time by the U.S. Securities and Exchange Commission in the 2017 DAO Report (SEC, 2017). On that occasion, the issue was resolved by applying the Howey Test, which defines the boundaries of an *investment contract* as a catch-all class of securities.[95] Under the Howey Test, developed by the U.S. Supreme Court in *SEC v. W.J. Howey Co.*, 1946, an investment contract for the purposes of the Securities Act means a contract, transaction, or scheme entailing (1) an investment of money (2) in a common enterprise (3) with a reasonable expectation of profits (4) deriving from the efforts of the promoter or of a third party.[96] The criteria established by the test allows the identification of those investment activities, characterized by financial risk and potential information asymmetries, which justify the applicability of security law requirements, such as the registration of a prospectus with the SEC, using a flexible and substantial approach.

Similar to the concept of *investment contract*, the category of *transferable securities* under EU law does not have fixed boundaries. Article 4(1)(44) MiFID defines transferable securities as "classes of securities which are negotiable on the capital market, with the exception of instruments of payment". The article provides an *explanatory* list of what constitutes a security, namely, (a) shares in companies; (b) bonds or other forms of securitized debt; and (c) "any other securities giving the right to acquire or sell any such transferable securities".[97] Similar to the approach set out by the Howey Test, EU Courts and financial authorities deploy a set of functional criteria to identify what constitutes a security for the purpose of MiFID and ancillary legislation. In particular, based on an interlinked reading of the Prospectus Regulation and of MiFID, securities are characterized by the features of tradability, negotiability on capital markets,[98] and standardization. Moreover, they need to present a functional comparability with other forms of security debt

95 (US) United States Securities Exchange Act (1934), Section 2(a)(36).

96 (US) SEC v. W.J. Howey Co., 328 U.S. 293 (1946).

97 Article 4(1)(44) of Directive 2014/65/EU.

98 ESMA, 'Prospectuses. Questions and Answers, 29th updated version – January 2019', ESMA (2019), https://www.esma.europa.eu/sites/default/files/library/esma31-62-780_qa_on_prospectus_related_topics.pdf, Q. 67: 'the essence of the definition of transferable securities in Article 4(18) MiFID is that, as a class, they are negotiable on the capital markets'.

(Hacker & Thomale, 2018), meaning, essentially, that they must incorporate a financial risk.

Transferability means the ability to transfer the ownership of the unit from one person to another, regardless of the existence of any documentation or registration of such ownership. Blockchains allow individuals to transact and store value in digital wallets protected by private keys; a person or entity having legitimate control of the private keys can prove ownership of the assets associated with the latter. Given that contractual restrictions do not suffice to exclude the transferability feature,[99] tokens will fulfill this requirement as long as their transferability is not precluded at a technical level.

Negotiability entails a de facto *capability of being treated* on a capital market.[100] Such capability is demonstrated by ongoing practices of crypto-assets trading. The ease with which tokens are traded on dedicated online exchanges shows their suitability to capital markets' modes of selling and buying.[101]

According to the CESR Technical Advice on the MiFID (CESR, 2010), standardization implies that issued units share a number of characteristics that allow them to be considered a homogenous class. To determine whether crypto-assets are sufficiently standardized, it does not matter that such assets, as a whole, do not constitute a homogeneous class of instruments. Standardization must be assessed at the level of individual issuers (Hacker & Thomale, 2018); tokens must be offered by a single issuer as standardized, fungible units (Hacker & Thomale, 2018). Hence, unless tokens are embedded

---

99 This follows from the wording of Article 7(7) of Regulation No. 2017/1129/EU, requiring information on contractual restrictions on the transferability of securities to be included in the prospectus and it is confirmed in ESMA, 'Prospectuses. Questions and Answers, 29th updated version – January 2019', ESMA (2019), p. 56: "the transferability of securities may be reduced on a contractual basis [. . .], ESMA considers that those securities remain "transferable securities" falling into the scope of the Prospectus Directive."

100 See: Financial Conduct Authority (FCA), 'Chapter 13: Guidance on the scope of MiFID and CRD IV', FCA (2019), https://www.handbook.fca.org.uk/handbook/PERG/13.pdf, Q. 28; and European Commission, 'Your questions on MiFID', European Commission (2008), https://ec.europa.eu/internal_market/securities/isd/questions/index_en.htm, Q. 115.

101 According to the EU Commission, even instruments that are not traded on a regulated market or MTF can be considered to fulfil the negotiability requirement (See: European Commission, 'Your questions on MiFID', European Commission (2008), Q. 115).

with claims and rights which make them individually different from each other, crypto-assets possess the feature of standardization.

Finally, to assess the last, functional requirement, an inquiry must be made into whether tokens resemble the types of transferable securities listed in MiFID by means of example, and whether they raise financial risks for investors so as to justify the applicability of prospectus rules. The answers to these questions need to be based on a case-by-case overview of issued crypto-assets. It is, however, a shared opinion that tokens can, in some situations, resemble shares or bonds (Hacker & Thomale, 2018), and they indeed present a financial risk which entails the need to mitigate information asymmetry (ESMA, 2019). This is confirmed, firstly, by the practice of publishing *white papers*, which have a similar purpose to that of prospectuses in enabling investors to make informed decisions. Secondly, the conclusion is reinforced by the rationale behind the exemptions set out in the Prospectus Directive. The regulator, in fact, estimates that the information asymmetry justifying the need for a prospectus is alleviated – and prospectus rules therefore do not apply – when securities are offered only to qualified investors or to a limited amount of investors (fewer than 150), or if the denomination per unit or the consideration per investor is sufficiently high (at least EUR 100,000).[102] ICOs, on the contrary, are typically addressed to very large crowds of retail investors, hardly ever accredited by professional intermediaries, and the consideration of each investor is normally very low. As such, crypto-assets offerings are diametrically opposite to those situations exempted from prospectus rules.

3.4.2 APPLICABLE LEGAL INSTRUMENTS AND ENFORCEMENT ISSUES

The qualification of crypto-assets as financial instruments brings them under the supervisory and regulatory competence of the European Securities and Markets Authority (ESMA), an independent EU authority responsible for the supervision of financial stability and investors' protection within the EU financial market. In light of its investor protection and supervisory convergence objectives, the Authority has put crypto-assets under its scrutiny,

102 Article 1(4) of Regulation No. 2017/1129/EU.

with the aim of identifying potential threats and suggesting the appropriate strategies for EU and national policymakers in its area of competence. Following a "substance-over-form" and "case-by-case" approach, the ESMA opens the possibility for crypto-assets to qualify as securities under the EU legal framework, and it establishes that, in such cases, the legal framework set out in MiFID II applies.

This view is in line with the principles that regulation should be technology-neutral and that the "same rules" should apply to the "same businesses". However, applying the MiFID legal regime might be easier said than done. Existing rules have not been drafted bearing in mind the specific features of crypto-assets, or the business models of the key intermediaries that are emerging in the ecosystem. Hence, supervisory and enforcement issues are likely to arise. The present section explores some of the EU legal instruments that become relevant when crypto-assets qualify as financial instruments, exposing related enforcement issues in the context of blockchain-based financial applications.

The Markets in Financial Instruments Directive framework

The Markets in Financial Instruments Directive framework (MiFID II) is composed of a directive (MiFID II), a regulation (MiFIR), and related implementing acts. The MiFID II framework establishes obligations for firms providing investment services/activities in relation to financial instruments as defined by the directive. In particular, under this framework, such firms need to be authorized as investment firms[103] by NCAs, and comply with specific requirements, including organizational, conduct of business, consumer protection, transparency, and reporting rules.

The applicability of MiFID II requirements to entities engaging with crypto-assets will vary depending on the type of service/activity provided, and the kind of financial instrument in question. In its advice, ESMA assesses the applicability of MiFID II to platforms involved with trading in crypto-assets. As these platforms perform trading and settlement in various

103 Article 4(1)(1) of Directive 2014/65/EU defines an *investment firm* as "any legal person whose regular occupation or business is the provision of one or more investment services to third parties and/or the performance of one or more investment activities on a professional basis".

ways, their legal treatment should be differentiated accordingly. A platform that keeps a central book and/or matches orders is likely to qualify as a *multilateral system*,[104] and should therefore operate as a Regulated Market (RM)[105] under Title III of MiFID II, or as Multilateral Trading Facility (MTF)[106], or as an Organised Trading Facility (OTF)[107] under Title II of the directive. Operators dealing on their own account and executing orders against their own capital – that is, acting like brokers/dealers – should instead comply with the requirements set out in Title II of MiFID II. Finally, platforms that are merely used to advertise buying and selling interests can be treated as bulletin boards, outside of the scope of MiFID II as of Recital 8 of MiFIR.

The ESMA recognizes existing barriers to the factual applicability of the MiFID II and MiFIR rules to firms operating in the crypto-assets market. For instance, the obligation to verify investors' reputation, trading ability, and competence is hardly compatible with the dominant practices of crypto-assets' trading venues. Since no professional intermediation takes place in crypto-assets' financial activities, the assessment should be carried out by the platforms/issuers themselves. Due to the large number of investors, such a task would be very resource-intensive. Moreover, as there is no formal entry barrier for investors (for example, no minimal threshold for the investment is normally set), it is likely that most participants lack the requisites to participate.

---

104 Article 4(19) of Directive 2014/65/EU defines a *multilateral system* as "any system or facility in which multiple third-party buying and selling trading interests in financial instruments are able to interact in the system".

105 Article 4(1)(21) of Directive 2014/65/EU defines a *regulated market* as "a multilateral system operated and/or managed by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments (...) in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules and/or systems, and which is authorised and functions regularly and in accordance with Title III of this Directive".

106 Article 4(1)(22) of Directive 2014/65/EU defines a *multilateral trading facility* (MTF) as "a multilateral system, operated by an investment firm or a market operator, which brings together multiple third-party buying and selling interests in financial instruments (...) in a way that results in a contract in accordance with Title II of this Directive".

107 Article 4(1)(23) of Directive 2014/65/EU defines an *organised trading facility* (OTF) as "a multilateral system which is not a regulated market or an MTF and in which multiple third-party buying and selling interests in bonds, structured finance products, emission allowances or derivatives are able to interact in the system in a way that results in a contract in accordance with Title II of this Directive".

Regulated markets and MTFs are normally registered in identified venues. Crypto-assets, on the other hand, can be issued and traded on websites without any legal entity's incorporation. This creates territoriality issues, further complicating the applicability of MiFID II requirements. As argued by Hacker and Thomale in relation to the applicability of the Prospectus Regulation, existing requirements "should apply if the website can be accessed, and tokens bought, from computers located in the EU" (Hacker & Thomale, 2018, p. 17). However, even when territorial competence can be established, it is unclear how competent authorities can carry out the necessary monitoring of platforms' conduct of business, detect infringements and enforce potential sanctions.

The most relevant issues arise in relation to platforms deploying decentralized business models and relying on self-executing pieces of code for their operations (so-called *decentralized exchanges*). While this emerging type of platform might mitigate traditional counterparty risks (ESMA, 2019), the fact that no accountable operator can easily be identified obstructs the enforcement of MiFID II requirements. Similarly, the ESMA identifies as problematic the qualification of hybrid platforms (for example, those that match orders but do not provide their execution), and the determination of the applicable rules.

The Prospectus Directive and Regulation

The Prospectus Directive,[108] and the more recently adopted Prospectus Regulation,[109] are key regulatory instruments aimed at ensuring investor protection by mitigating information asymmetry within the EU financial market. In particular, the prospectus regime requires the approval and distribution of a prospectus "when securities are offered to the public or admitted to trading on a regulated market situated or operating within a Member State",[110] unless specific exemptions apply. Precisely, the prospectus rules apply to regulated secondary markets "situated or operating within a Member State",[111] and

108 Directive 2003/71/EC.

109 Regulation 2017/1129/EU.

110 Article 1 of Regulation 2017/1129/EU.

111 Article 1(1) of Directive 2003/71/EC and Article 1(1) of Regulation 2017/1129/EU.

to entities issuing securities in the EU, even when incorporated in a third country and not listed in regulated secondary markets in the EU.[112]

Under the Regulation, the prospectus must contain all the information that is necessary for investors to make an informed assessment of the financial situation of the issuer and/or of guarantors, of the rights attached to the securities, and the circumstances of the issuance. Before publication, the prospectus must be approved by the competent national authority, and it will be valid across all EU Member States.

Where crypto-assets qualify as transferable securities, their issuers and trading platform operators – if located or operating in the EU – are obliged to fulfill the prospectus requirements. This conclusion seems to find confirmation in the reasoning behind the exceptions to the obligation of publishing a prospectus provided in Article 1(4) of the regulation. Beside the case in which the size of the offer does not trigger the applicability of the legal instrument,[113] the legislator exempts operators from prospectus requirements when: (a) securities are offered solely to qualified investors; (b) the offer of securities is addressed to fewer than 150 natural or legal persons per Member State, other than qualified investors; (c) the denomination per unit of the security amounts to at least EUR 100,000; and (d) the offer of securities is addressed to investors who acquire a consideration of at least EUR 100,000 each. These circumstances are unlikely to take place in the context of ICOs, which tend to gather a large number of participants that contribute with small amounts of funds. As mentioned above, token sales often take place in the very early stages of the project, and in the absence of intermediaries (such as registered Credit Rating Agencies[114]) that can verify the suitability of the issuer. This increases the possibility of scams and unsuccessful business initiatives. Hence, the rules established by the Prospectus Directive and Regulation are suitable for the crypto-assets industry, where the need to tackle information asymmetries is real.

---

112 When issuers are incorporated in a third country, they must be assigned a "home Member State" and obtain an approval that will be valid across the EU.

113 See: Article 1(4) of Regulation 2017/1129/EU.

114 See: Regulation 1060/2009/EU; Regulation 513/2011/EU; Regulation 462/2013/EU.

The need for crypto-assets' public sales to be accompanied by detailed and transparent information is demonstrated by the established practice of drafting white papers. A white paper is a document published on a project's website normally containing basic information on the issuer, the structure of the token offer (initial price, amount of offered tokens, etc.), the implementation roadmap of the project, and some technological details.

White papers are generally free in form and content, and subject merely to the scrutiny of retail investors. The Prospectus Regulation, on the other hand, provides for highly standardized formats of prospectus and summary documents. Since, as of today, no specific schedule is provided for the public offer of crypto-assets, the ESMA advises that prospectus schedules should be used in a flexible manner, and that the concept of *adapted information* should be applied (ESMA, 2018). For instance, if an ICO is considered to substantially resemble an IPO, the issuer could be required to comply with the information requirements that are set out for equity securities. Moreover, the disclosure of the code underlying the crypto-asset in question could become mandatory for prospectus purposes (OECD, 2019).

Notwithstanding the formal applicability of the law, however, the enforcement of prospectus requirements on blockchain-based ventures faces several challenges. The violation of prospectus requirements is the basis upon which the Italian financial supervisory authority, CONSOB, has recently ordered the suspension of two public offers of tokens – which the authority qualified as de facto *financial instruments* – to Italian investors.[115] The case revealed important enforcement drawbacks as: (a) the infringement was detected solely on the basis of private reporting; and (b) the suspension of the order was executed due to the cooperation of the Internet Service Provider (in this case, Facebook), which agreed to shut down the webpage where the token sale was addressed to Italian investors.

Book-entry forms, bookkeeping and recordkeeping requirements

Businesses providing services for crypto-assets' storage and transaction shall also be subject to book-entry form requirements, rules on safekeeping, and

115 CONSOB, delibera n. 20740/2018 | CONSOB, delibera n. 20741/2018.

recordkeeping of ownership and rights attached. For instance, issuers of crypto-assets could – if the digital asset in question qualifies as a security and is traded on a trading venue – be obliged to ensure that such securities are represented in book-entry form with authorized Central Securities Depositories (CSDs), as defined under Article 2(1) of the Central Securities Depositories Regulation. The applicability of rules on safekeeping and recordkeeping of ownership of securities is, however, unclear in the context of crypto-assets. First, Regulatory Technical Standards[116] used for reporting and recordkeeping obligations are based on identifiers and classifications that do not capture crypto-assets, so they will likely need to be adapted to such new instruments (ESMA, 2019). Secondly, there is no EU-wide definition of what constitutes safekeeping and recordkeeping activities, and the related rules apply to a variety of actors such as custodian banks, registrars, notaries, depositaries, and CSDs. Finally, it is not clear what constitutes safekeeping in the specific context of crypto-assets. The ESMA is of the opinion that holding private keys on behalf of clients might be regarded as a safekeeping activity, triggering the applicability of related rules. However, further clarification is necessary as the control of private keys can be shared among multiple actors, such as in the case of *multi-signature wallets* where more than one key is needed for transactions' validation.

In a recent guidance, the U.S. Financial Crimes Enforcement Network (FinCEN) clarified the applicability of the Bank Secrecy Act (BSA) obligations – which include recordkeeping, recording, and transaction monitoring – to business models that involve money transmissions in *convertible virtual currencies* (FinCEN, 2019[117]). Examining a number of exemplary business models, the document highlights that "P2P exchangers are required to comply with the BSA obligations that apply to money transmitters, including registering with FinCEN as an MSB [money service business] and complying with AML program, recordkeeping, and reporting requirements".

---

116 European Securities and Markets Authority (ESMA), 'Regulatory technical and implementing standards', ESMA (2015), https://www.esma.europa.eu/sites/default/files/library/2015/11/2015-esma-1464_annex_i_-_draft_rts_and_its_on_mifid_ii_and_mifir.pdf, Annex I MiFID II / MiFIR.

117 Financial Crimes Enforcement Network (FinCEN), 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001', FinCEN (2019), https://www.fincen.gov/resources/sta tutes-regulations/guidance/application-fincens-regulations-certain-business-models.

With regard to wallet providers, the analysis distinguishes between *hosted wallets*, wherein funds are controlled by a third-party service provider, and *unhosted wallets*, wherein users themselves control the funds. While hosted wallet providers must comply with AML and monitoring obligations that apply to money transmitters, unhosted wallet providers are generally exempted

from such rules. The document also considers the case of *multiple-signature wallet providers*, which typically "maintain in their possession one key for additional validation, while the wallet owner maintains the other private key locally" (FinCEN, 2019, p.17). Also in this case, the key distinction is between hosted and unhosted wallets, which determines the providers' control over the stored value: "If the multiple-signature wallet provider restricts its role to creating un-hosted wallets that require adding a second authorization key to the wallet owner's private key in order to validate and complete transactions, the provider is not a money transmitter because it does not accept and transmit value. On the other hand, if the person combines the services of a multiple-signature wallet provider and a hosted wallet provider, that person will then qualify as a money transmitter" (FinCEN, 2019, p. 17).

The FinCEN guidance suggests the importance of looking at the actual technical capabilities and level of control exercised by the service provider in order to attribute the appropriate degree or type of legal responsibility. In line with these criteria, actors that do not store transactions in privately controlled servers or do not manage users' private keys may be exempt from requirements around book-entry forms, bookkeeping, and recordkeeping. More generally, to define which rules should govern the operations and technical procedures of financial operators, it seems fundamental to look at the technical infrastructure that underpins transactions, and the ways in which it shapes the interactions between the involved parties. The attribution to users of greater control over funds and the public accessibility of blockchain's transactions' records might make some of the rules provided for book-entry forms, bookkeeping, and recordkeeping redundant.

Legal framework on crowdfunding

Within the EU legal framework, crowdfunding is an activity covered by specific rules – currently being reformed by the European Commission. Crowdfunding

is defined by the ESMA as "a means of raising finance for projects from 'the crowd' often by means of an internet-based platform through which project owners 'pitch' their idea to potential backers, who are typically not professional investors".[118] Based on such a definition, ICOs and token sales can, in many cases, be qualified as a form of crowdfunding.

Currently, the rules applicable to crowdfunding vary significantly across Member States. In general, it is possible to distinguish between more traditional and more "innovative" approaches. Whereas the former bring *financial return crowdfunding* under the scope of banking or financial regulation, the latter deploy bespoke regimes or safe harbors (Ferrarini & Macchiavello, 2018). In general, the dominant approach across the EU is that of establishing, for crowdfunding activities, exemptions from financial market rules; however, these are not easily applicable because of strict caps limitations.[119]

To eliminate differences across the Capital Market Union and foster the development of the emerging crowdfunding industry, the European Commission – as part of its 2018 Fintech Action Plan – has presented a proposal for a regulation on crowdfunding service providers.[120] The proposal has the scope to ease access to alternative (non-bank) sources of finance, "such as crowd and peer-to-peer finance ('crowdfunding')"[121] for innovative companies, start-ups and other unlisted firms. In particular, the new rules apply to crowdfunding services which entail a financial return for investors, such as investment and lending-based crowdfunding.[122]

Considering the likelihood of Initial Coin Offerings and crypto-assets sales to be deployed in the context of crowdfunding activities, the European

118 European Securities and Market Authority (ESMA), 'Opinion on Investment-based crowdfunding', ESMA (2014), https://www.esma.europa.eu/search/site/Opinion%2520investment-based%2520crowdfunding?within_ doc1⁄41&solrsort1⁄4&perpage1⁄420.

119 See: Rohr J., Wright A., 2017. The article analyzes the U.S. crowdfunding regulation and argues that existing caps ($1 million per 12 months) make crowdfunding exemptions unsuitable for ICOs.

120 See: Proposal for a regulation of the European Parliament and of the Council on European crowdfunding services providers (ECSP) for Business, COM(2018) 0113 final.

121 Commission legislative proposal for an EU framework on crowd and peer to peer finance, COM(2018)113.

122 Proposal for a regulation of the European Parliament and of the Council on European Crowdfunding Service Providers (ECSP) for business, COM(2018) 0113 final.

Commission should clarify the applicability of the new legal framework – which will also include amendments to MiFID II – to intermediaries involved in blockchain-based peer-to-peer financing. The new regulation, in fact, could provide a coherent supervisory system and a unified licensing regime for blockchain-based crowdfunding initiatives.

3.5 PAYMENT TOKENS

A separate, but interconnected, area of regulation that could apply to blockchain-based crypto-assets – and firms in this area of business – is that pertaining to banking and payment services. In 2019, the European Banking Authority (EBA) – competent for the supervision and prudential regulation of the European banking sector – issued an assessment on the potential applicability to crypto-assets of rules governing electronic money and payment service providers. In particular, its recently published 'Report with advice for the European Commission' (EBA, 2019) addresses the question of whether crypto-assets that are used as a means of payment may qualify as *electronic money*, falling under the scope of the Electronic Money Directive 2 (EMD2),[123] and of the Payment Services Directive 2 (PSD2).[124]

The report responds affirmatively: when crypto-assets are used as a means of payment, they can qualify as *electronic money* within the meaning of the EMD2. Such a qualification implies that the assets in question are also to be considered *funds* for the purposes of the PSD2. It follows that firms offering *payment services* (as listed in Annex I of the PSD2) in crypto-assets fall within the scope of the PSD2. According to this Directive, Member States must ensure that electronic money is issued only by authorized *electronic money issuers* (Article 10 PSD2) and that these have in place appropriate resources (including an initial capital of at least EUR 350,000 and a proportionate amount of their own funds), and safeguarding measures.

---

123 Directive 2009/110/EC of the European Parliament and of the Council of September 16, 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, repealing Directive 2000/46/EC, [2009] OJ L 267/7 (Electronic Money Directive 2).

124 Directive 2015/2366/EU of the European Parliament and of the Council of November 25, 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, [2015] OJ L 337/35.

The application of Anti-Money-Laundering rules is also a main concern regarding cryptocurrencies used as a means of payment. Notably, the Anti-Money Laundering Directive[125] has been recently amended to include virtual currencies-to-fiat exchanges and custodian wallet providers in its scope of application. However, the Financial Action Task Force (FATF, 2012)[126], ESMA (ESMA, 2019), and EBA (EBA, 2019) have all underlined that the Directive needs to be further updated to include the wider spectrum of actors involved in the crypto-assets industry, namely: a) providers of crypto-asset to crypto-asset exchanges, and b) providers of financial services for ICOs.

Concerning institutions (credit institutions and investment firms), payment institutions and electronic money institutions that engage in activities involving crypto assets (such as owning crypto-assets, making markets, lending against crypto-asset collateral, providing custody or exchange services, etc.), the EBA report highlights the priority of establishing adequate reporting and disclosure requirements. Moreover, it advises the Commission to promote as much as possible "convergence on the accounting treatment of institutions' exposures to crypto-assets". The EBA is also conducting a study on the prudential treatment of banks' exposure to/holding of crypto-assets in cooperation with the Basel Committee on Banking Supervision,[127] assessing the need to establish capital and liquidity requirements. In the meantime, the Authority advices that policymakers and institutions – both at the EU and at the national level – should adopt a conservative, prudential approach in order to mitigate risks arising from exposure to crypto-assets.

Finally, the EBA acknowledges the lack, in most jurisdictions, of specific reporting obligations for crypto-assets' activities. Therefore, it announces

---

125 Directive 2015/849/EU of the European Parliament and of the Council of May 20, 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015] OJ L 141/73.

126 Financial Action Task Force (FATF), 'International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations', FATF (2012), http://www.fatf-gafi.org/publications/fat frecommendations/documents/fatf-recommendations.html.

127 See: Bank for International Settlements (BIS),'The Basel Committee on Banking Supervision – overview',BIS(2020), https://www.bis.org/bcbs/index.htm.

the development of a *common monitoring template* that national authorities can provide to institutions for them to report their activities in this domain.

In the document analyzed here, the EBA advances the opinion that existing supervisory powers should suffice to provide oversight and take timely action on possible risks to the financial soundness of the regulated entities. The report, however, was published before the announcement by Facebook of the upcoming launch of Libra, a new digital currency designed to run on a private blockchain governed by a consortia of e-commerce platforms and payment firms. The proposal of Libra, in fact, revived discussions within EU institutions on the need to fill existing gaps in the regulation of crypto-assets (Jones, 2019), and to assess the related risks, "in particular with regard to financial stability, monetary policy, data privacy, money laundering, consumer protection, competition and cyber security".[128]

3.6 CONCLUSIONS

This chapter presented some of the most relevant legal instruments that apply to crypto-assets and related activities under European financial law, exposing the challenges of enforcing existing rules to fluid, ever-evolving and possibly ephemeral financial applications based on DLTs. Such analysis is useful to identify important policy questions for further research, and to inform the current debate on the need for regulatory intervention at the EU level in this domain.

From a conceptual and methodological point of view, European authorities determine the legal treatment of tokens by including them within general categories – payment, investment and utility – that are associated with different, specific functions. These three categories, designed to steer crypto-assets toward specific areas of regulation, are to be considered *archetypes*, whereas existing tokens tend to combine more functions (hybrid tokens) and present fluid characteristics. Therefore, while this classification is important, it does not avoid the need to adopt a case-by-case approach when evaluating risks and legal provisions that concern crypto-assets.

---

128 European Parliament, 'Parliamentary question n. E-002268/2019', European Parliament (2019), http://www.europarl. europa.eu/doceo/document/E-9-2019-002268-ASW_EN.html.

Crypto-assets that qualify as investment instruments or as electronic money fall under the scope of European financial regulation. Specifically, the requirements for issuing and trading securities apply to tokens with an investment component, while the rules governing e-money and payment service providers are applicable to payment tokens. However, such a simplistic scheme has several weaknesses. The attempt to bring crypto-asset investments under existing safeguards and investor protection schemes is justified by concrete risks, but the overview provided in this chapter shows that current requirements do not always fit the features of businesses and start-ups in the blockchain industry – their technical, operational processes, as well as their inherent incentive systems.

On the one hand, some concepts and requirements need to be better defined and understood in the context of DLTs; for instance, it should be clarified what constitutes "custody or safekeeping of crypto-assets". On the other hand, the application of existing requirements is likely to be hindered by enforcement issues, which arise because of decentralization, the international nature of DLTs, and non-incorporation of entities. Finally, not all tokens can be captured, based on their specific functions, by existing legal regimes. This is the case for crypto-assets that are commonly referred to as utility tokens. In order to fill the legal vacuum, some EU Member States (as of today: Malta, Gibraltar, Lichtenstein, and France) have put in place bespoke legal regimes to ensure a coherent, comprehensive legal framework for the growing industry. However, a fundamental problem persists: the line between security, payment, and utility tokens is blurry. Legal regimes might overlap or succeed each other in different phases of the tokens' lifespan. For this reason, legal uncertainty remains a major issue, as tokens are functional parts of evolving, innovative solutions which can hardly be reduced to pre-existing classes or defined a priori.

Beyond these shortcomings in the applicability of existing rules, a normative stance on the regulation of blockchain-based financial applications must also take into account the socio-economic dynamics that shape and are re-shaped by these technologies, checking them against the policy objectives that regulation tries to achieve. The issue of how existing legal requirements and safeguards should be applied within the DLTs ecosystem is primarily a question about the roles of the various actors involved therein. The recent announcement by Facebook about the creation of its own, privately controlled "global currency

and financial infrastructure that empowers billions of people"[129] is a good reminder of the need to scrutinize the interests and powers that drive the development of blockchain-based solutions.

Despite its decentralized, open-source roots, the crypto-asset market got quickly populated by a whole new range of intermediaries and financial service providers – that is, exchanges, custodian wallet providers, cryptocurrency landing platforms, remittances services, and investment funds managers – which, due to their business models and organizational/technological arrangements, might not be covered by current legal definitions, and/or may be able to elude supervisory regimes. With this in mind, the regulation of blockchain-based financial applications must not only be concerned with fighting illicit behaviors, but also with balancing conflicting interests at stake and preventing influential actors from taking advantage of legal loopholes and institutional failures.

The regulatory and technical enforcement challenges posed by DLTs epitomize a broader, ongoing struggle between technological change and law's efforts to follow. From New York's "BitLicence" and the Chinese ban, to the Maltese ad-hoc legal framework, the regulatory attempts that have been seen so far demonstrate that regulation plays an important role in directing the development of the technology: the practices it enables, its geography and public adoption. Yet, defining a legal framework for emerging blockchain-based financial technologies is a task with no stable or durable solution, as there are multiple, colluding, and evolving iterations of blockchain-based value transfer applications.

The principle of technological neutrality entails treating the "same businesses with the same rules". At the same time, however, the appreciation of the (purported) social and economic potential of DLTs is inciting policymakers (themselves attracted by profit opportunities) to relieve innovative businesses from burdensome legal duties constructed for older kinds of economic actors.

Should financial law requirements be better tailored to accommodate decentralized business models and peer-to-peer fintech solutions? Why are

129 Libra Association (2020) 'White Paper'.

some states particularly interested in attracting the blockchain industry? What are the advantages and what are the dangers of blockchain-based, privately managed financial networks? Is a "regulatory competition" among states – aimed at attracting the industry – potentially beneficial, or could it jeopardize legal safeguards, creating risks for financial stability, market integrity, and consumer protection? Is legal intervention necessary to protect an adequate level of competition in the provision of financial services within the EU? These are some of the long-term policy questions that legal scholars, and European as well as national lawmakers, must address to navigate the uncertain terrain of the regulation of crypto-assets.

CHAPTER 4: THE PLATFORMIZATION OF VALUE TRANSFER INFRASTRUCTURES: RETRACING SOCIO-TECHNICAL IMAGINARIES IN THE EUROPEAN POLICY AGENDA

4.1 INTRODUCTION

Organized around banks' APIs and mediated by tech companies, payment infrastructures are reshaped as digital platforms aimed at maximizing data production and valorization. Such a process of *platformization* of financial services is likely to bring about issues typically associated with platform business models (Poell et al., 2019), and information capitalism (Cohen, 2019). Yet, while financial innovation is widely discussed from advantaging business perspectives, it is rarely scrutinized in terms of information control-related risks, power asymmetries, and the negative externalities of platformization.

This chapter uses discourse analysis to investigate how sociotechnical imaginaries influence the fabrication of the notion of consumer interest in policy-making around the digitalization of payments, and how the latter is mobilized to justify policy choices.

Section 4.2 introduces the issue that is central to the policy agenda analyzed here: the process of platformization of digital payment infrastructures. Specifically, it draws a critique of platforms as infrastructures (4.2.1), explains how payment services are becoming a new digital industry (4.2.2), and illustrates the European policy that is enabling this change. Section 4.3 explains the notion of *socio-technical imaginaries* and its relevance in the exploration of policy discourse (4.3.1). Sub-section 4.3.2 outlines the role of

consumer interest as justification in policy discourse. Section 4.4 explains the methodology, which consists of a systematic qualitative analysis of policy documents issued by EU institutions (the Commission, the Parliament, the European Banking Authority, the European Central Bank and two technical bodies) in the area of fintech and, more specifically, digital payments, starting from the 2017 Fintech Resolution and the following 2018 Fintech Action Plan until today.

Section 4.5 reports the findings of the qualitative analysis, illustrating, in 4.5.1, the sociotechnical imaginaries of digital payments as they emerge from the corpus of selected documents, and, in 4.5.2, the notion of *consumer interest* that is mobilized in the policy discourse to justify the process of platformization of payment services. Finally, section 4.6 provides a critical analysis of such findings, arguing that the notion of consumer interest portrayed in the documents is based on assumptions – identified through the discourse analysis as part of the sociotechnical imaginaries – that are partially constructed.

The thesis of this chapter is that there are two main fallacies in the policymakers' discourse on digital payments. The technologies that are portrayed as desirable are chosen based on industry interests and trends rather than on a scrutiny of the benefits and risks that these technologies imply for consumers. Moreover, the assumption that a liberalized market will offer more and better choices is flawed, as the platformization of the digital payment industry entails the risk of monopolization and abuses of market power. The mobilized notion of consumer interest – anchored to the rhetoric of consumer technological empowerment – outweighs and conceals much-needed considerations about the vulnerability of consumers in the context of data-intensive technologies and the platform economy.

We conclude by suggesting that policymakers in this domain should be more attentive to the risks that are emerging in adjacent digital industries, and open their imagination to alternative technological futures.

4.2. THE PLATFORMIZATION OF THE DIGITAL PAYMENT INFRASTRUCTURE

4.2.1 INFRASTRUCTURES AS PLATFORMS

The present paper is concerned with the *platformization* of the digital payment *infrastructure*. The term *infrastructure* is generally used to refer to sociotechnical systems, or technological assemblages, that underlie or support public interest, universal or quasi-universal services (Plantin et al., 2018). The traditional notion of infrastructure saw these systems as centrally created and controlled, organized as public or semipublic monopolies. This so-called "modern infrastructural ideal", however, collapsed in the 1970s with the liberalization and deregulation of many infrastructures based on neoliberal stances on free competition and market efficiency (Plantin et al., 2018, p. 300). This meant the replacement of public, centrally organized infrastructures with "fragmented, privatized yet interoperable systems and services" (Plantin et al., 2018, p. 300).

The design and the governing model of infrastructures reflect particular political-economic choices. The notion of "infrastructure" is in fact scrutinized across various academic disciplines – including Sociology (Mukerji, 2010), International Political Economy (Bernards and Campell-Verduyn, 2019; Bellanova and de Goede, 2021), and Anthropology (Larkin, 2013) – as the domain of power exercised through invisible, non-transparent technological devices and architectures. They are investigated as material assemblages in which political choices, and dynamics of oppression and exclusion, are embedded and transferred upon social and economic exchanges. A specialized domain of study, Critical Infrastructure Studies, has emerged, which brings infrastructures within the domain of humanistic enquiry, understanding them not only as technical skeletons but also as conditions and vehicles for cultural experiences and expressions in late modernity. This latest conceptualization becomes salient in the context of expanding information infrastructures and cyber-infrastructures which, in the past three decades, have come to organize and define all areas of cultural and economic interactions.

The concept of *platform* shares some features with that of *infrastructure*, but it is useful, from an analytical point of view, to distinguish between the two. Both concepts refer to a technical system which serves more salient

activities performed on top of it. Platforms have been defined across a variety of disciplines as firms, markets, or data infrastructures. Poell et al. describe them as "(re)programmable digital infrastructures that facilitate and shape personalised interactions amongst end-users and complementors, organised through the systematic collection, algorithmic processing, monetisation, and circulation of data" (Poell et al., 2019, p.2). From a technical point of view, they are technical systems composed of low variability core components which allow applications to be built on top, using complementary components. From an economic point of view, "platforms constitute two sided, or increasingly, complex multi-sided markets that function as aggregators of transactions amongst end-users and a wide variety of third parties" (Poell et al., 2019).

The platform ecosystem expands quickly with the inclusion of third-party service providers abiding by platforms' technical and economic standards (Plantin at al., 2018). Centralizing control over data across multiple services and unilaterally setting rules across entire portions of the market, platforms gain competitive advantage and power; exploiting global scale network effects, they easily establish market monopolies across multiple industries and jurisdictions (van Dijck et al., 2019).

The expansive nature of platforms determines the enclosure of more and more substrata of infrastructural systems within the platform ecosystem. Scholars point out that many infrastructures are undergoing a process of platformization (Plantin et al., 2018). The process of *platformization* has been defined as the "penetration of infrastructures, economic processes and governmental frameworks of digital platforms in different economic sectors and spheres of life, as well as the reorganization of cultural practices and imaginations around these platforms" (Poell et al., 2019, p.1). The concept is mostly deployed to criticize the increasingly central role taken up by globally operating businesses platforms such as Google, Facebook, Amazon, and Uber in all aspects of social, economic, cultural, and political life. While the latter is more accurately referred to as the "infrastructuralization of platforms", "platformization" also refers to the specular phenomena of the reorganization of existing infrastructures in the form of platforms.

A critical approach anchored on platform studies looks at the relationship between agency and architecture, against the background of a particular

political economy. Understanding the ongoing changes in the digital payment ecosystem as a shift at the infrastructural level, and, more specifically, as a process of platformization, directs the attention toward the power relationships that are typical of platform economies, and demands a consideration of technological affordances and design options in light of the logics of accumulation and expansion which characterize the latter.

4.2.2 THE EMERGING DIGITAL PAYMENTS ECOSYSTEM

The platformization of the payment infrastructure is the substitution of a pre-existing assemblage of actors, material infrastructures, and processes with a digital platform ecosystem (Langley et al., 2021). This entails the representation of money in the form of digital data (Mejias, 2019) that can be captured and valorized within the digital platform architecture (Sadowski, 2019), and the reorganization of financial interactions around digital platforms (Mattila et al., 2018).

Payment services are increasingly bundled within platform ecosystems, which leverage integrated data pools to establish dependencies across large portions of markets, and to scale across jurisdictions. On one side, banks allow this penetration, providing technology companies with access to financial data networks (through APIs), and outsourcing services and functionalities to technology providers. On the other, technology companies expand their businesses by adding payment functionalities, which allow them to "embed financial transactions within their data streams" (Westermeier, 2020, p. 2).

Established digital platforms position themselves between payers and financial institutions, incorporating payment functionalities in their ecosystems (Westermeier, 2020; Mattila et al., 2018). This is the case for Apple Pay and Google Pay, for instance. In this model, the digital service provider collaborates with existing payment institutions. By offering users frictionless, seamless, and convenient means to initiate transactions, tech companies ensure that transaction data are produced within the platform. The key element here is that of authentication: users do not need to go through additional steps when paying with their smartphones, as the platform already has the means in place to verify their identity. This raises concerns about power and information concentration in the hand of a few big global corporations; such concerns

are particularly worrying in light of the huge data analytics potentials of transaction data when interlinked with other data points held on big digital platforms (Ferrari, 2020).

Tech-driven companies also provide intermediation between the financial infrastructure and businesses. Westermeier discusses the example of solarisBank, which is termed a banking-as-a-Service platform, allowing non-bank businesses to provide financial services to end customers, using solarisBank as a bridge to financial infrastructures (Westermeier, 2020, p. 8). This model is incentivized by the PSD2, which enhances the role of APIs as points of access to financial data streams for third party service providers (Berber & Atabey, 2021). This paves the way to a financial service industry in which interaction with consumers is shifted from banks to non-bank digital service providers; while the latter capture consumers' data, banks fall into the background, becoming invisible to consumers.

Finally, the penetration of the tech industry within the financial domain comprises initiatives that, by completely bypassing existing financial infrastructures, introduce newly built networks on top of which users can transact digitally native currencies. Digital currencies based on blockchain technologies have initially been developed by tech-savvy individuals and groups of developers with anarcho-libertarian aims. Around cryptocurrencies, a market has developed including digital currency exchanges, investment firms, and a continuous stream of software and hardware releases. The hype around blockchain-based financial technologies has also stimulated experimental adoptions of national digital currencies (what are termed Central Banks Digital Currencies), as well as digital currencies backed and controlled by private parties. A notable example of the latter is the *stablecoin*[130] Libra (now renamed Diem), a currency designed by Facebook and intended to be used for payments within and outside the platform's ecosystem. The project, announced in 2019, received a push back from regulators and is being re-evaluated by the company. However, the idea of leveraging blockchain technologies for the creation of digital payment infrastructures is still popular in both the public and private sectors (Westermeier, 2020, p. 8).

130 *Stablecoins* are virtual currencies, the value of which is asset-backed (in physical collateral or crypto-assets) or algorithmically controlled in order to avoid price fluctuations typical of non-fiat digital currencies.

4.2.3 THE EUROPEAN POLICY ON FINTECH AND DIGITAL PAYMENTS

European policymakers have been explicit about their intention to open up the financial sector to tech-driven companies. In 2016, the European Commission set up a Financial Technology Task Force "to help FinTech innovation reach its full potential" (Commission, 2016). The European Parliament, in its 2017 Resolution on Fintech, acknowledged the potentials and risks of "the influence of technology on the future of the financial sector and called [upon] the Commission 'to draw up a comprehensive FinTech Action Plan' to foster the development of FinTech" (European Parliament, 2017). Following a Public Consultation in 2017, the Commission launched its Fintech Action Plan in 2018: a broad policy agenda whose aim is to "enable the EU financial sector to make use of the rapid advances in new technologies that are transforming the industry and revolutionizing the way people access financial services" (Commission, 2018). In particular, the Action Plan has a threefold goal: 1) enabling innovative business models to scale up at the EU level using common standards and interoperable solutions; 2) supporting the uptake of innovation in the financial sector by ensuring the absence of legal obstacles to the adoption of new technologies; and 3) enhancing the security and integrity of the financial system.

A central pillar of the broader fintech policy agenda is the promotion of a European digital payment market. The PSD2 is the key legal instrument setting the conditions for the liberalization of this market; entered into force in 2018, it expanded the scope of PSD to new types of internet-based payment intermediaries, and it established banks' obligations to share customer data with third-party service providers (Donnelly, 2016).

The technical steps for the promotion of a European digital payment ecosystem are directed and supervised by the Euro Retail Payments Board (ERPB), a "high level strategic body" chaired by the ECB. Created in 2013, the ERPB comprises representatives "from the demand side" (consumers, retailers and corporations) and "from the supply side" (banks and payment and e-money institutions), as well as representatives from national central banks. [131] Since

131 See: https://www.ecb.europa.eu/paym/groups/erpb/html/index.en.html.

its launch, it has worked on the promotion of: 1) pan-European instant payments; 2) payment initiation services; 3) peer-to-peer mobile payments; and 4) contactless payments. Since 2017, the ERPB has been meeting the chairs of EU national payment committees in the European Forum for Innovation in Payments (EFIP)[132], another informal forum initiated by the ECB and the Commission to facilitate the exchange of information between the various stakeholders involved in restructuring the digital payment ecosystem.

In January 2020, the Commission published an updated Work Program titled "A Union that strives for more", announcing its intention to launch a new action plan on FinTech before the end of 2020. On September 24, 2020, following a consultation with stakeholders, the Commission released a Communication on a digital finance strategy, confirming its commitment to support digital transformation in finance. In the document, particular attention is given to digital payments, as it is recognized that they play a "key role among digital financial services, being at the cutting edge of innovation and instrumental to support the digital economy" (Commission, 2020). Beside the ongoing efforts to consolidate and standardize existing payment schemes, the Commission and the European Central Bank (ECB) announced, in early 2021, their cooperation on the development of a digital euro (ECB, 2021). The digital euro project was officially launched in July 2021 with the aim of investigating, for the first 24 months, "key issues regarding design and distribution" of the digital euro architecture (ECB, 2021).

4.3 SOCIOTECHNICAL IMAGINARIES AND JUSTIFICATIONS AS ANALYTICAL DISCURSIVE ELEMENTS

4.3.1 THE ROLE OF SOCIO-TECHNICAL IMAGINARIES IN HIGHLY TECHNICAL FIELDS OF POLICYMAKING

Formulating policy always requires, to some extent, making predictions about the future. This is particularly true when the aim is to regulate technologies that are yet to be materialized, or that are in the process of transformation. The design of policy agendas demands the mobilization of a certain vision of the future: an expected threat, or a desired outcome. When policymaking regards complex scientific issues or technological developments, the delineation

132 See: https://www.ecb.europa.eu/paym/groups/efip/html/index.en.html.

of that desired outcome is highly dependent on the imaginaries, hopes and fears that are attached to the technology or scientific phenomena in question.

According to Mager and Katzenbach, "evocations of possible or fantastic, desirable or dystopian futures are necessarily genuine sociopolitical processes with material consequences in the present" (Mager and Katzenbach, 2020, p.2). Visions of the future are not only imagined but, when properly located and promoted, they are "concretely constructed"; imaginaries are *performative* in as much as they induce the materialization of future prospects in the present.

The concept of "socio-technical" or "future imaginaries" has been deployed in several studies as an analytic tool to identify the "collectively held and institutionally stabilized" (Jasanoff and Kim, 2009) visions of the future that mobilize the coproduction of techno-scientific projects and policy. Where the development and regulation of digital technologies is concerned, studies have shown that influential tech companies propagate assumptions about technology which reflect the design of their products (Mager and Katzenbach 2020; Markham, 2020).

Recent studies have explored the role of industry-driven sociotechnical imaginaries in the ongoing development of digital payment infrastructures (Mützel, 2021; Vidan 2020). These studies, as well as similar studies conducted in other fields (Haupt, 2021; Liao and Iliadis, 2021), demonstrate that sociotechnical imaginaries are largely produced by corporations promoting specific technological design and functionalities. In my analysis, I identify and offer to the reader the vision of the future of payments as it emerges from the words of policymakers. Linkages between this vision and external sources that might have influenced the institutions' imagination (such as private actors' promotion of technological choices) are not established, nor can they be extracted directly from the text; yet, deploying the concept of sociotechnical imaginaries already implies the possibility of that link.

The policy-making agenda that is the object of the present study is highly future-orientated. The digital payment infrastructure presented in the policy documents is in large part yet to be materialized. Consequently, the policy agenda that is analyzed in this paper is partially a story about a future to be built, and partially a manual of instructions for its realization.

For this reason, I deploy the concept of "sociotechnical imaginary" as a thinking tool to highlight the speculative nature of certain descriptions and expectations, and to recall the notion that the prospected vision of the future is determined by a given discourse, chosen amongst other multiple possible futures.

4.3.2 CONSUMER INTEREST AS JUSTIFICATION IN PROCESSES OF LIBERALIZATION

For the purpose of the textual analysis, this chapter identifies policy *justifications* as a distinctive discursive element that intersects with, but performs different functions from, the sociotechnical imaginaries. While the latter consists of narrative, imaginative visions about what the digital payment ecosystem *will* look like, justifications are articulated as normative arguments. Appealing to considerations of necessity, efficiency and benefits, justifications are pragmatic considerations which motivate and corroborate the idea that a particular future *should* materialize.

In EU policymaking discourse – particularly in relation to processes of market liberalization and deregulation (Cseres, 2008; Reisch and Micklitz, 2006) – a central justification for policy action is the realization of consumer interest (Lynggaard, 2019). Adopting regulation requires balancing the rights of consumers/citizens with the prerogatives of businesses; in such a balancing exercise, a precise notion of a consumer is developed. Such an image is necessarily fictional: it is a simplification of reality which collapses together a heterogeneous mass of individuals which in fact differ in terms of preferences, needs, and capabilities (Mak, 2015, p. 381). Such a fictional image of the consumer permeates and influences policymaking processes as an agent that benefits from, promotes, or participates in economic and social exchanges that are the object of regulation.

In EU consumer law, two main conceptualizations of the consumer inform the rules that govern the relationship between "persons acting as consumer in the marketplace and their counter-parts, the businesses" (Wilhelmson, 1998, p.4). On one side, the "paternalistic model", developed in the 1960s and '70s (Cseres, 2005, p. 321), sees the consumer as a vulnerable subject who needs legal protections against violations of their rights, interests, and safety

in the context of asymmetrical contractual relationships with businesses. On the other, the neoliberal, rational, empowered consumer acts as a "sovereign market actor" (Helberger et al., 2013, p. 7), as long as she is granted the necessary information and bargaining power to do so. The latter assumes that free market competition produces the best conditions for consumers to exercise their economic decisions, and invokes a *laissez-faire* approach with minimal state intervention, as opposed to the more interventionist paternalistic approach (Cseres, 2005, p. 322).

Recent developments in EU law have demonstrated that the digital economy has induced a reappearance of the earlier conceptualization, revealing the shortages of the neoliberal dogma according to which free market competition and consumer interest go hand in hand. The EU Commission 2020 New Consumer Agenda[133] stands in sharp contrast to the 2012 European Consumer Agenda:[134] whereas the older document cites the "digital revolution" as a source of economic gains for consumers, the 2020 document recognizes how digital transformation limits the effectiveness of consumer protection rules. The latter, in fact, states that in digital commercial applications, "the underlying data collection and processing combined with analysis of consumers' behaviour and their cognitive biases can be used to influence consumers to take decisions that may go against their best interests" (EU Commission, 2020, p. 10).

The need for a more interventionist agenda resulted in the adoption of several consumer protection-related legal instruments specifically addressing issues of the digital economy. The specificity of the position of consumers in the digital space was recognized by the Digital Content Directive[135] (Helberger et al., 2013, p. 8) and the Directive on Better Enforcement

133 EU Commission, Communication From The Commission To The European Parliament And The Council New Consumer Agenda Strengthening Consumer Resilience For Sustainable Recovery Com/2020/696 Final (New Consumer Agenda).

134 EU Commission, Communication From The Commission To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions A European Consumer Agenda - Boosting Confidence And Growth /* Com/2012/0225 Final (European Consumer Agenda).

135 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content. COM/2015/0634 final - 2015/0287 (COD).

and Modernisation of Consumer Law.[136] Recently, a decisive signal has been given with the proposal for a Digital Services Act (DSA),[137] aimed at creating "a safer online experience for citizens [...] and ensuring the protection of fundamental rights" online. Importantly, the DSA recognizes the power imbalances between platforms (especially "very large online platforms") and their users (including both business users and consumers); hence, it establishes a "transparency and accountability framework for online platforms", setting out oversight and enforcement mechanisms to counter manipulative and unfair practices of digital intermediaries.[138]

The peculiarity of users' status in digital environments depends on the conditions under which they interact with and within digital ecosystems. Digital environments work in ways that are obscure and non-transparent to their users, creating inherent information asymmetries. Users engage with digital environments based on technical affordances, tasks and patterns that are predefined by the digital ecosystem provider; the algorithmic processes that determine the provision of services are concealed behind friendly interfaces.[139] This inherent information asymmetry, cumulated with the informational power that digital companies derive from data, creates opportunities for service providers to speculate on users' personal vulnerabilities. Personal and behavioral data, in fact, is used to nudge users' behavior and influence users' decision-making through, for instance, personalized offers and prices (Janssen et al., 2020, p.13).

Information asymmetries and risks of manipulation – which are inherently present in commercial digital applications (Sax, 2021) – undermine the image

---

136 Directive (EU)2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (OJ L 328, 18.12.2019, p. 7).

137 Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

138 For instance, by establishing transparency obligations regarding online advertising (Art. 24) and regulating the use of recommender systems (Art. 29).

139 The relevance of information exposure on platforms' interfaces is recognized by the DSA, at Recital 62: "A core part of a very large online platform's business is the manner in which information is prioritized and presented on its online interface to facilitate and optimise access to information for the recipients of the service".

of the consumer which is foundational to a liberal approach to consumer protection. The consumer as a sovereign, rational, active market actor gives way to a vulnerable, passive user in need of protection. Updating existing legal frameworks as to address the challenges of digitization requires, therefore, a re-conceptualization of the digital consumer as an agent whose choices are nudged and technically pre-determined by the techno-social system that surrounds them.

The push toward the digitalization and platformization of the payment ecosystem is a push toward both the liberalization of the market and the integration of the new service industry at the EU-wide level. Processes of liberalization are traditionally justified as means to realize the interest of consumers (Micklitz and Weatherill, 1993): according to the neoliberal axiom, increased competition will bring down prices and grow the possible choices for consumers. Not surprisingly, the realization of consumer interest is a core justification in the policy agenda analyzed here. But what image of the consumer is mobilized? A strong, free market player or a vulnerable actor? Which needs, priorities and interests are taken into consideration?

The present chapter investigates which image of the consumer is mobilized by European policymakers to justify the liberalization of the digital payment industry, and which sociotechnical imaginaries influence the fabrication of such an image.

4.4 METHODOLOGY: RETRACING SOCIOTECHNICAL IMAGINARIES AND JUSTIFICATIONS IN POLICY DISCOURSE

Discourse analysis as a method of inquiry is aimed at looking at "discourse" as a "specific ensemble of ideas, concepts, and categorizations that are produced, reproduced and transformed in a particular set of practices through which meaning is given to physical and social realities" (Hajer, 1995). This methodology is devoted to the question of how collective systems of meaning are built, which power relationships they constitute, and which knowledge, practices, and literacies they imply and produce.

The policymaking agenda that is the object of the present chapter is highly future-oriented. The digital payment infrastructure presented in the policy

documents is in large part yet to be materialized. Therefore, the policy agenda analyzed in this chapter is partially a story about a future to be built, and partially a manual of instructions for its realization. For this reason, I deploy the concept of *sociotechnical imaginary* as a thinking tool to highlight the speculative nature of certain descriptions and expectations, and to recall the notion that the prospected vision of the future is determined by a given discourse, chosen among other, multiple possible futures.

For the purpose of the textual analysis, this paper identifies policy *justifications* as a distinctive discursive element that intersects with, but performs different functions from, sociotechnical imaginaries. While the latter consists of narratives, and imaginative visions about what the digital payment ecosystem *will* look like, justifications are articulated as normative arguments. Appealing to considerations of necessity, efficiency, and benefits, justifications are pragmatic considerations which motivate and corroborate the idea that a particular future *should* materialize.

The boundaries of discourse as an object of analysis are fluid. Identifying the material which forms the object of the analysis, and selecting one way of reading and interpreting such material, are choices which remain open to criticism. Whichever variation of the method we select, it can never exhaust the possible paths of interpretation, association, deconstruction, contextualization, and even delimitation of what we identify as discourse. In my analysis, I choose to focus on official documents produced and published by European institutions and publicly invested bodies involved in the making of the European payment infrastructures.

4.4.1 CORPUS OF DOCUMENTS

The methodology of this chapter consists of a systematic qualitative analysis of policy documents issued by EU institutions in the area of fintech and, more specifically, digital payments. The most significant policy documents setting a general agenda for fintech developments within the EU are the European Parliament 2017 Fintech Resolution and the Commission 2018 Action Plan on Fintech, with annex publications. Moreover, I analyze a selection of documents produced by the European Banking Authority (EBA) and by the ECB, both of which are involved in the design of the digital

payment infrastructure and its legal framework. The latter documents have been chosen either by virtue of reference from other documents, or through a snowball search on the institutions' websites using the keyword "digital payment(s)". The results of the search (which produced 403 results for the EBA, and 1224 for the ECB) have been automatically sorted by relevance and manually scanned in order to select a manageable and representative sample of relevant documents representing the positions of the two institutions on the issue at stake in the years taken into consideration for the purpose of this study. Concerning the EBA, particular attention is paid to the Working Group (WG) on APIs under the PSD2.

The corpus also comprises documents produced by two expert groups specifically tasked with "fostering the integration, innovation and competitiveness of euro retail payments in the European Union" (ECB, 2021): the Euro Retail Payments Board (ERPB)[140] and the European Forum for Innovation in Payments (EFIP)[141]. These two multi-stakeholder technical bodies are relevant as forums where substantial, technical issues concerning the development and governance of the digital payment infrastructure are discussed.

The PSD2 is the legal instrument which regulates the provision of digital payment services within the EU. The current debate and policymaking activities regarding digital payments consequently revolve around the implementation and the potential need to update the PSD II, and/or implement other regulatory measures to facilitate a pan-European, integrated digital payment infrastructure. Notwithstanding its importance within the regulatory framework, the PSD2 has been excluded from the corpus as the goal of the study is to investigate the discourse *after* and *beyond* the PSD2 – how the industry and the institutional discussion seeks to move further.

The corpus is therefore composed of 41 documents, from 6 institutions, covering the period from 2017 until the first half of 2021 (see Annex 1). With this selection, the intention is to provide a representative picture of the dominant discourse on digital payments as it is made publicly available by the institutions that are involved in designing its legal framework. To cover

140 See: https://www.ecb.europa.eu/paym/groups/erpb/html/index.en.html.

141 See: https://www.ecb.europa.eu/paym/groups/efip/html/index.en.html.

all the relevant documents is beyond my capabilities and resources; therefore, I acknowledge the limited scope of the inquiry, and the possibility of having overlooked material that should have been taken into consideration.

4.4.2 CODING

All the documents have been analyzed using the qualitative content analysis software Atlas.ti. The process involved the full reading of each document, and simultaneous manual annotation and coding of the text. After all documents were analyzed, the codes were reorganized, merged into groups and put in relation to each other to find patterns of associations and threads within the discourse. This exercise implied a process of repeated back and forth reflection between the authors' annotations, the codes, and the text itself. The list of the code groups, and the relative sub-codes associated with each group, can be found in Annex 2.

Circumscribing narrow areas of discourse and identifying key terms, the coding process helped understand the structure of the discourse across the various institutions and document types. Using the coding tree, it was possible to find discursive patterns, overlaps or interrelations of concepts and terminology to identify the various issues around which the analysis is structured. A limitation of this methodology is the unavoidable influence of a researcher's goals, perspective, and sensitivity to some topics, or words, rather than others. This limitation is partially overcome by coding the text as comprehensively as possible, regardless of whether the information is deemed to be more or less relevant for the analysis.

4.5 FINDINGS

In this section I explain the findings of the analysis. First, I illustrate the sociotechnical imaginaries of digital payments as they emerge from the corpus of selected documents (4.5.1). I organize this section by identifying the most relevant issues emerging from the corpus of documents and systematizing them under different subsections; the organization under separate topic areas supports the clarity of the explanation, and these topic areas are, in reality, intertwined with and co-dependent on each other. In 4.5.2, I retrace the notion of consumer interest that is mobilized in the

policy discourse to justify the process of platformization of payment services, identifying two main conceptualizations of such a notion: empowered vs. weak consumer/user.

4.5.1 SOCIO-TECHNICAL IMAGINARIES OF DIGITAL PAYMENTS

4.5.1.1 DATA COMMODIFICATION

European institutions have put the construction of a European digital payment infrastructure at the core of their digital finance strategy. This is stressed in several documents which highlight the strategic role of digital payments for the contemporary EU economy.

Once relegated to the back-office, payments have become strategically significant. They are the lifeblood of the European economy (CommComm2020).

The value of the digital payment industry is boosted by the monetization of transaction data; this implies that the payment service industry is reorganizing itself as a data-intensive technological industry, with the breaking up of pre-existing value chains. Regulators understand that technological companies, interested in the data generated by financial transactions, have infiltrated and reshaped the market. As the technical infrastructures and the logics of value production governing the digital payment market evolve around data monetization, the networks of actors involved in the provision of payment services moves dynamically and beyond the agency of regulators, remodeling services through new technologies:

Technology is contributing to breaking up previously integrated value chains […] *as new entrants adopt new business models leveraging technology such as application programming interfaces (APIs) and platforms* (CommCons2021).

Data produced in the context of financial transactions is highly informative of people's private lives, tastes, behaviors, and movements. Because of the sensitive nature of financial data, its strategic role for law enforcement, and the economic opportunities attached thereto, the governance of the technological system underpinning payment networks becomes a primary concern for policymakers. For this reason, the structuring of the backbone infrastructure, the licensing rules for service providers, and the data-access

requirements governing financial networks are to be determined by the policy agenda.

The need for institutional control, however, is counterweighted by a highly neoliberal attitude aimed at exploiting the economic opportunities offered by digital payments data flows: "to scale up innovative finance in Europe a free flow of data within the Union is needed" (EPRes2017).

European policymakers are, therefore, first and foremost concerned with creating the conditions for European technology companies to profit from this growing data market; this market-oriented attitude is reflected in the PSD2, the aim of which is to enable data flows from banks to technology companies.

4.5.1.2 LIBERALIZATION AND COMPETITION

EU institutions envision a competitive market where fintech companies can grow and provide users with better and cheaper payment services, which are interoperable and reachable across national borders: "[…] enhancing competition and leading to more choice, better services, as well as lower prices for over 500 million consumers" (CommCons2017).

Payment services' EU-wide reach is a central prerogative for the policy agenda: enabling cross-border transactions without additional fees, and generating EU-wide data value chains, is necessary for EU companies to compete with large non-European platforms serving European citizens. To this aim, the policy agenda seeks to eliminate national constraints to cross-border transactions, and facilitate pan-European reach with the imposition of common standards. For example, the documents stress the need to guarantee technology companies access to payers' accounts data according to the rules and mechanisms that are valid across the whole Union.

The policy documents emphasize the role of the private sector, in particular technology companies, in shaping the digital payment ecosystem of the future. Private entities are tasked with developing critical technological infrastructures providing payment functionalities to users and businesses across the EU. "The Eurosystem will continue to support private initiatives for retail payments" (ECBPress2020).

The documents express confidence in the development of European payment solutions through the establishment of a liberalized, innovation-friendly market which would leverage the potentialities of platforms, i.e., the bundling of multiple services and service providers within a single technical infrastructure. While guaranteeing European autonomy from foreign actors in the short term, a competitive European digital payment ecosystem can, in the long run, gain global reach, increasing European geopolitical influence. There are five key objectives: "pan-European reach, customer friendliness, cost efficiency, safety and security, European identity and governance, and, in the long-run, global reach" (ECBPress2020).-

The role upheld by EU institutions is, therefore, that of facilitating this privately led "digital (re)evolution," coordinating and supervising the development of the industry, while safeguarding the fundamental interests of the Union. Bringing payment services up to date with the digital transformation occurring in other domains demands efforts to ensure that various risks – "in terms of money laundering, financing of terrorism, cyber-attacks, as well as operational and liquidity risks for financial institutions" (CommComm2020) – are tackled with supervision and adequate legal safeguards, including consumer protection and risk mitigation measures. This precautionary approach is needed to establish consumers' trust in technological solutions, as necessary for their widespread uptake.

If not appropriately identified and addressed, these risks may undermine the confidence of consumers and merchants using instant payments, potentially hindering their full rollout as the new normal (CommComm2020).

4.5.1.3 PLATFORMIZATION

As organizational structures that conjoin a plurality of services and markets, the concept of the platform is central to the policy agenda on fintech. European policymakers envision the realization of a pan-European digital payment platform, capable of connecting EU-based financial and non-financial service providers operating across member states.

In today's global, internet-based economy, payment services must be able to interconnect multiple services, industries and markets; they must be

infrastructures with a tentacular reach, giving users the ability to interact (purchase, transact, and receive money) with any party from a single interface and mobile device. Being by definition two-sided or multi-sided markets, payment services in the digital commerce ecosystem are prone to be organized as platforms.

According to the EBA, a digital platform/platform enables at least one financial institution directly (or indirectly using a regulated or unregulated intermediary) to market to customers, and/or conclude with customers contracts for, financial products and services within the EEA (CommReq2021).

The documents acknowledge that the payment industry is undergoing a process of platformization; this is to both organize financial data networks around banks' APIs, and to merge payment services with the broader ecosystem of technology platforms – and their data streams – that operate in and structure digital markets in other domains.

[We recognize the] *importance of APIs, as a complement to other tools that can be used by the consumer, in providing new actors with access to financial infrastructure* (EPRes2017).

Platformization is, therefore, a change occurring at the infrastructural level: an organizational model shaping networks of relationships and distribution of power among the actors moving in the financial sector. It also entails the centrality of data as the main revenue source of the industry, with data access being the first requisite for market entrance, and data availability the condition to compete. By positioning mobile applications between financial networks and users, moreover, platformization entails a particular type of literacy and affordances for the users of payment services.

The infrastructural precondition for the realization of a digital payment platform connecting the European market is EU-wide standardization of tools and processes for digital payments. This requires ensuring service providers' compliance with common standards and adherence to uniformly applied

rules, under the supervision and control of financial supervisory authorities. Key for cross-European standardization is the uniform development and

implementation of APIs. An API is defined as "a set of rules and specifications followed by programmes to communicate with each other, and an interface between different programmes that facilitates their interaction" (CommReq2021). The role of APIs is that of linking services and applications, and establishing the connectivity of products with customers and partners by managing data access. APIs are key nodes in platform ecosystems as they enable the "bundling of various financial services, often from various service providers such as payments services, payment accounts, lending, investment, and insurance products" (CommReq2021).

Determined to "unlock the potential of open banking beyond PSD2", the ERPB seeks to concretize the vision of a pan-European digital payment platform bundled through the establishment of a "Single Euro Payments Area (SEPA) Application Programming Interface (API) access scheme encompassing services beyond the (mandatory) scope of PSD2 by following a non-regulatory, coordinated approach aim[ed] at addressing the mutual interests of the stakeholders" (ERPBreact2020). As infrastructural, non-regulatory intervention providing concrete benefits for industry stakeholders, this is considered by institutions, including the Commission and the EBA (CommComm2020), as a key instrument for the removal of obstacles to the realization of open banking as envisioned by the PSD2.

APIs are the gates that define rules of access to service providers' databases. Which data is transmitted depends on the components of digital identity and authentication requirement standards – another priority area of the policy agenda. Also on this matter, the primary concern is to establish pan-European harmonization: cross-national and cross-sectorial recognition of authentication requirements and techniques. Financial institutions are called to ensure interoperability and ease of use of digital identity and authentication techniques (CommComm2020). The interoperability requirement is necessary for the uptake of mobile payment services and for the linkage of payments to other services within digital platforms: users must be able to interact with their finances using, instead of IBANs, credentials that are readily available through third parties' services (EFIP2019).

The uptake of European payment solutions, however, faces one fundamental obstacle that the free-market logics followed by the Commission are not able

to circumvent. The Commission recognizes that large technology companies located abroad are already ahead in the process of introducing payment functionalities within their platforms' environments. Large non-European technology companies can exploit their market dominance to overtake the provision of payment services within the EU, further consolidating their platform monopolies. The Commission voices the concern that these companies might establish themselves as dominant players in the field of digital payments in the EU. They could, in fact, profit from network effects and global reach to gain a dominant position in the EU market, stifling competition from European technology providers.

Large technology providers can use their customer data and network effect advantages to enter the payments sector, leveraging their market power from social media or search services (CommComm 2020).

According to the European institutions, large technology platforms pose regulatory challenges for two reasons: first, they are likely to generate competition issues; second, as they perform both regulated and unregulated activities, they require the supervision of different authorities and cross-sectorial, coherent oversight efforts.

[We] *need to break down supervisory silos across sectors, and recommend close cooperation by financial sector supervisors with other relevant national and European bodies that have the required technological expertise* (EPRes2017)

Developing a domestic digital payment ecosystem is, therefore, also a protectionist, defensive strategy against the spectrum of foreign bigtech and "technologies governed abroad", which threaten to undermine European sovereignty and the protection of individual rights.

The expansion of big tech companies could make us dependent on technologies governed elsewhere (ECBInt2021)

However, little is said about how domestic companies will effectively be favored over foreign ones. Promoting wide scale and transnational reach, in fact, the policy ultimately favors bigger technology providers over smaller local ones, and does nothing to challenge the strategic position held by U.S.-

based companies (PayPal, Google, Apple) which already provide payment functionalities to EU citizens. The dependence on U.S.-based companies might turn out to be a hard-to-eradicate feature of the payment industry (think of plastic cards as well).

In a world increasingly dominated by digital platforms, large technology providers are taking advantage of their vast customer base to offer front-end solutions to end-users. Their entry into finance may consolidate the network effects and their market power (CommComm2020).

4.5.1.4 TECHNOLOGICAL TRANSFORMATION

Technological development is depicted as an exogenous, unstoppable phenomenon which will inevitably impact the way financial transactions are performed and managed. The technological revolution has already started: the technological affordances provided by dominant market players are here to stay, and they already inform the needs of citizens, as well as the future direction of the industry.

Customers' expectations of 'seamless' payments, ongoing consolidation and the redesign of payment platforms and market infrastructures contribute to a transformation in payments (EBARep2019).

The digitalization of money and payments is depicted as a "natural evolution" in the context of a ubiquitous digitalization of commerce and communication.

A digital euro represents a natural evolution in response to this transformation (ECBInt2021).

Changes in business models and market structures, the entrance of new actors (technology providers not previously engaged with the financial service industry), and shifts in the governance of money are unavoidable, as means of payment need to adapt to the surrounding socio-technical ecosystem. Policymakers can only acknowledge and participate as facilitators of the process, trying to steer it within the parameters of what is deemed desirable according to European regulatory principles. In this perspective, incentivizing the emergence of a European digital payments industry through liberalization and regulatory

incentives is a strategy to bring technological development into the proximity of EU institutions, to keep it closer to their domain of agency.

There is a considerable dose of techno-solutionism in the way policymakers surrender to the imperative of technological evolution. Their view seems to subscribe to an ageless Californian ideology according to which governments should "stay off the backs of resourceful entrepreneurs" (Barbrook, Cameron, 1996, p.6), who will enable useful technological progress in a competitive marketplace. The struggle, then, is to reconcile this ideology with European values and the commitment to make technological services inclusive and democratic.

The goal of the liberalization process is to pave the way for an innovative and competitive digital payment market providing services based on cutting-edge technologies:

> *A number of factors are expected to contribute to a further acceleration of this innovation* […] *the development of new technological innovations such as Big Data analytics, artificial intelligence and robo-advice* (EBARep2017).

Technological development will allow the creation of a digital payment ecosystem that is *accessible*, *inclusive*, and *interoperable* across borders. A number of technologies are expected to reshape the ways we transact and interact with our finances: AI, robotics, blockchain, cloud, and mobile technologies are among the most quoted. These technologies are meant to support *faster*, *cheaper*, and *safer* means of payments and enable frictionless interactions with financial incumbents. Technological applications will provide *cash-like functionalities*; they will be *consumer-centric*, *user-friendly*, and *seamless*.

Payments are envisaged being performed mostly via mobile devices, through proximity and contactless technologies. Authentication techniques will increasingly rely on biometrics rather than passwords. Automation and robotics will improve compliance processes and multiple aspects of the relationship with consumers. Institutions are also enthusiastic about the possibilities of data analytics to personalize products, financial offers, and service conditions based on the specific needs of consumers.

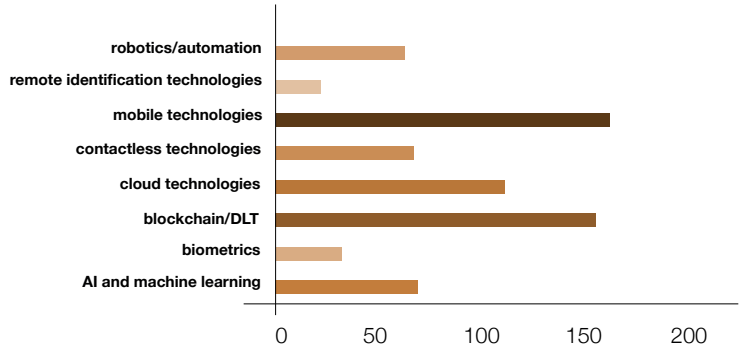

Fig. 5: Mention of specific technologies in the analyzed corpus of documents. Source: elaborated bythe author based on Atlas.it data.

This enthusiasm for technological innovation is not always counterbalanced with inquiries about the limitations of these technologies. No mention is made, for example, of the well-documented technical limitations of blockchain and distributed technologies.[142] Institutions rather superficially mention issues associated with the application of AI for automated decision-making for the management of personal finances,[143] including discrimination and unfair pricing, but their potential benefits seem to overweight such risks. The political and legal problems related to the international nature of technological artifacts' supply chains (for instance, that mobile technologies are mostly produced in China and in the U.S.) are omitted from the discussion, as well as the effects of digitization on labor conditions (Jones, 2021) and policies.

4.5.1.5 REGULATION AND SUPERVISION

The policymaking agenda collected for the purpose of the present discourse analysis is highly future-oriented: it envisions and depicts a digital payment infrastructure that is yet to be fully materialized. The role of regulation is to *facilitate* the materialization of that vision.

142 See: Monrat A. A., Schelén O., Andersson K., (2019) "A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities," in *IEEE Access*, vol. 7, pp. 117134-117151, reporting the shortcomings of blockchain technologies in terms of scalability and performance, interoperability, privacy, energy consumption, security, and legal compliance.

143 See: Eubanks, V. (2017). *Automating inequality: how high-tech tools profile, police, and punish the poor*. New York: St. Martin's Press, about the far-reaching negative consequences of automated decision-making in public services.

The declared goal of European institutions is to ensure that the Union will benefit from the affordances of cutting-edge, data-intensive technologies and the economic possibilities offered by them. Policymakers are committed to *enable,* through various regulatory and technical interventions, the growth of the digital payment industry. Institutions' intention is to set the direction for the private sector to modernize, and optimize the ways payments are performed through information technologies, riding the *momentum* of fintech, pursuing a *vision* of development and change. Their approach is aimed at ensuring the *preparedness*, *fitness*, and *readiness* of Europe for the digital age. Technological progress is unstoppable and unavoidable; hence, the task of institutions is to set a framework within which new technologies can flourish. There is an "importance of boosting financial innovation in Europe" (EPRes2017). Furthermore,

> *Today's Action Plan envisages* [...] *enabl[ing] the financial sector to make use of the rapid advances in new technologies, such as blockchain, artificial intelligence and cloud services* (CommPress2018).

The policy agenda is characterized by a pressing tone, resembling an accelerationist manifesto stressing the need to *harness*, *reap*, *untap*, *boost*, *accelerate*, and *fuel* the benefits of fintech and the digital transformation of finance. Urgency and speed are the core temporal elements in the policy agenda. Institutions must *catch up* with the technological revolution, moved partially by genuine optimism about the affordances of new technologies, and partially by a "fear of missing out" on changes that will overwhelm them.

One could wonder about the rationale of this strategy: delegating digital payments to a liberalized marketplace of technology companies equates to the self-destruction of pre-existing legal structures and of the national monopoly on money circulation. However, upon closer look, the chosen policy direction must be read within the frame of a presupposed technological determinism which forces institutions to *adapt* to an ongoing technological disruption. Digitalization and liberalization are unavoidable choices if the EU economy wants to survive the fierce global competition among tech corporations to harvest the data of a globally wired population.

The need for regulation to "reap the benefits of fintech innovation" translates into precise regulatory principles and key actions. First of all, regulation in

the financial domain needs to maintain an innovation-friendly outlook, encouraging industry-led solutions and allowing spaces for self-regulation.

The purpose of the digital finance strategy is to ensure that the EU regulatory framework for financial services is fit for the digital age. This includes enabling the use of innovative technologies and making the framework compatible with prevailing best practice in software production and deployment (CommComm2020).

This translates into soft regulatory measures such as innovation hubs and regulatory sandboxes, as well as regulatory frameworks for the use of specific technologies such as AI and Cloud Computing – all measures aimed at favoring the adoption of new technologies from the financial sector's service providers. Importantly, key for the realization of the policy is the correct implementation and appropriate amendment of the PSD2. The EU Commission, in fact, is committed to facilitate, with legal and technical guidance, the correct implementation of the rules regarding data flows as set out in the directive.

The Commission aims to ensure through regular legislative reviews and interpretative guidance that the EU regulatory framework for financial services neither prescribes nor prevents the use of particular technologies while also ensuring that regulatory objectives continue to be met (CommComm2020).

Another principle that is often mentioned is that of technological neutrality, meaning the idea that regulation must tackle activities and services, not technologies. In other words, it should be the: "same activity, same risks, same rules" (CommComm2020). The aim is to "ensur[e] a technology-neutral and innovation friendly EU financial services regulatory framework" (CommCons2021).

This principle seems to be at odds with some of the proposals of the policy agenda, such as that of issuing a regulation on crypto-assets and blockchain-based tokens – technologies which still have to stabilize their use, function, and legal relevance.

The issue with regulating rapidly changing technological solutions for the financial sector, as it emerges in several documents, is, first of all, a temporal

one. It is, in fact, often stressed that rules, guidelines, and interpretations cannot be static, but must be updated on a regular basis. This is the so-called "future-proofness" of the regulatory agenda: in order not to hamper innovation, regulation must be constantly re-tailored and re-clarified based on the latest, ongoing technological developments.

Through regular reviews, the Commission will ensure that potential material regulatory obstacles to innovation stemming from legislation on financial services are removed. It will regularly provide interpretative guidance on how existing legislation on financial services is to be applied to new technologies (CommComm2020).

One of the elements imposing regular regulatory updates is the rapid change not only of technologies, but also of the actors and their functions within the ecosystem: "The financial ecosystem is becoming increasingly complex with a more fragmented value chain. The payments chain involves many players (some regulated, others not) and increasing levels of complexity and inter-dependency" (CommComm2020). A crucial point in the policy agenda is, therefore, that of establishing clear licensing and authentication schemes, bringing up to date the list of actors that are covered by the PSD2.

As payment services increasingly rely on the provision of ancillary services by or on outsourcing arrangements with unregulated entities, the Commission considers it indispensable to assess, in the context of the PSD2 review, whether some of these services and providers should be brought into the regulated sphere and be made subject to supervision (CommComm2020).

A counter-narrative to the "boosting innovation" approach incorporated in these regulatory principles is the emphasis on the risks brought by technological change. Without abandoning the innovation-friendly mindset that illuminates the whole agenda, institutions recognize that the complexity and variegated nature of the emerging ecosystem requires balancing different interests:

While regulation must guarantee a level playing field, promote fair competition and low barriers to entry and spur innovation, it must also uphold users' rights and protect the overall ecosystem from financial and operational risks. To achieve these objectives, the regulatory perimeter needs to be well balanced (CommComm2020).

Specifically, it is argued that "the increased use of customer data or big data by financial institutions", and "the increasing combination of personal data and algorithms", while they "may lead to benefits to consumers", can also cause "systemic risk and harm consumers, for example through increasing exclusion" (EPRes2017). To such risks, and to issues deriving from "errors or biases in algorithms or in the underlying data", as well as the "misuse/non-disclosed use of data", the main solution that is identified is "to ensure that adequate regulation [i]s in place and enforced to protect individuals" (EPRes2017). Particular mention is made of the GDPR, and the rights enshrined within in:

The provisions of the GDPR, which grant the data subject the right to obtain an explanation of a decision reached by automated processing and to challenge this decision […] *guarantee that incorrect data can be changed and that only verifiable and relevant data are used; [and] calls on all stakeholders to increase efforts to guarantee the enforcement of these rights [...C]onsent given to the use of personal data needs to be dynamic and [...]data subjects must be able to alter and adapt their consent* (EPRes2017).

The prudential approach is translated into enhanced supervision and oversight of the payment ecosystem; because of the pace of technological change, the Commission explains, supervision requires appropriate skills and constant training of the supervisors.

Supervision and oversight of the relevant actors in the payments chain has become increasingly complex, taking into account the emergence of many new business models and group structures. The potential supervisory implications became apparent in a recent case involving a technology company providing payment-related services (CommComm2020).

Such skills and training critically require cooperation between "regtech providers, financial players and regulators" (CommComm2020). Supervision becomes complex because the entrance of non-financial actors into the industry breaks up traditional supervisory silos and causes different areas of competences to spill over each other. "Players in the payments chain may be under the supervision or oversight of different entities" (CommComm2020). Furthermore:

Large technology companies offer a wide range of services and have elevated intra-group dependencies, for instance on integrated data pools, operating systems and processes, and customer access. They may use their vast amount of customers' data to support the provision of financial services giving rise to questions about conduct and prudential risk management, which have not been present so far in traditional mixed activity groups. These taken together suggest that they pose risks of a more systemic dimension. Hence a holistic approach to their supervision may be necessary (CommReq2021).

This cooperative and cross-sectorial approach, referred to as "multidisciplinary supervision" (CommCons2021), implies supervisors' dependence on the tech industry's expertise. Supervisors' training needs to rely on the private actors responsible for technology development and implementation. This raises questions regarding the capacity of supervisors to critically assess, for example, the real necessity of a technological feature, the risks it entails, and its future development.

4.5.2 THE FABRICATION OF CONSUMER INTEREST

Beside appeals to future imaginaries, policy choices are motivated through arguments of necessity, and benefits – pragmatic considerations that justify the efforts toward the materialization of that particular future. Justifications are key to institutional discourse as they legitimize policy choices. By identifying both future imaginaries and the arguments that are deployed by policymakers to justify a given direction of action, this analysis serves to highlight the links, the overlaps, and mutual influences between the two discursive elements. In the policy documents, we identify the realization of consumer interest – defined either as consumer empowerment or as consumer protection – as the central justification for policy choices.

4.5.2.1 CONSUMER TECHNOLOGICAL EMPOWERMENT

The policy agenda encourages the entrance of technology companies into the financial domain, so that, though fair competition, a digital payment industry can develop and offer products which best meet consumers' needs and expectations with regard to digital payments.

Mobilizing the realization of consumer interest as a justification for policy action implies developing a precise notion of what is needed or desired by a hypothetical model consumer. In the documents, there seem to be precise assumptions about which technological features correspond to consumers' needs and desires when it comes to payment technologies: "faster, cheaper, more tailor-made, more inclusive, more resilient and more transparent and better financial services" (EPRes2017). These expectations are shaped by the technological affordances that digital technology providers have established as default options for digital environments: personalization, friendly interfaces, and interoperability among services within a single platform.

Customers now demand fast, cheap, easy, smooth and secure payments at any time and from anywhere, and seek more options and choices (EBARep2019)

Consumers are assumed to desire the latest, most advanced technological solution offered by the market. Meeting consumers' needs, therefore, amounts to enabling them to make use of the technological solutions offered by tech companies, establishing a co-dependency between the latter and the traditional financial sector. In other words, technology companies are better suited to providing what consumers need. There is, therefore, an assumption that a liberalized market populated by competitive tech companies, making the best use of financial data, will produce what is in the best interests of consumers.

This line of reasoning serves as a justification for the promotion of collaborations between new technology providers, such as Account Information Services and Payment Initiation Services, and banks, as "access to more customer data would also enable service providers to offer more personalized services that are better tailored to customers' specific needs" (CommComm2020). It is also the rationale behind the transition of "consumer ownership" from the banks to technology providers: the latter provide the interfaces, defining users' modes of interaction with their finances, and determining the types of literacies that are necessary for using financial technologies.

But the rhetoric of consumer empowerment through increased datafication also responds well to the interests of technology companies. Many fintech

applications adopt *freemium models*[144] and exploit data for various commercial purposes: marketing, insurance, credit scoring, etc. (Ferrari, 2020). The *user experience* in digital apps is designed with the goal of multiplying the data points linked to users, informed by the algorithmic personalization of services and advertising (Janssen et al., p. 13). A "better", personalized user experience, therefore, is not only aimed at responding to consumers' needs – as policymakers seem to understand – but it is, first of all, functional to the data-intensive business models that technology companies adopt.

4.5.2.2 CONSUMER PROTECTION

The consumer/user plays a central role in the rhetoric used to justify the policy agenda in two ways: on the one hand, as seen above, as a market actor interested in market efficiencies and empowered by innovations; and on the other hand, as a vulnerable actor to be protected from the negative externalities of digital services.

While companies claim to be using data analytics to optimize the digital environment in order to respond to the needs of individual users,

> *data could be mis-used to target vulnerable consumers; companies can exploit data in non-transparent ways to apply dynamic pricing techniques or encourage, through personalised offers, frivolous spending or hyperconsumerism* (EBARep2017).

The main threats demanding a focus on consumer protection in the development of the digital payment industry relate to data protection, cybersecurity, and digital illiteracy. With regard to the first, it is acknowledged that digital financial transactions entail the production and management of highly informative personal data, and these data are likely to be abused for commercial purposes.

According to the ECB, "the abuse of personal information for commercial or other purposes could endanger privacy and harm competition" (ECBInt2020).

144 Monetization models in which the app is free to download and use, but users can pay to enhance their experience through in-app purchases or subscriptions; often, this model also relies on advertising as source of revenue. See: Sax, 2021.

This position seems to be at odds with the rest of the agenda, which promotes data-intensive business models as essential economic strategies. Moreover, the line between legitimate commercial use and abuse of personal data is not clearly drawn. Linking to the GDPR *modus operandi*, mention is made of the necessity of user consent to the processing of personal data. However, in the context of an essential service such as digital payments, using consent as discriminating criteria for legitimate data processing misses the point. In fact, as digital means of payments are increasingly becoming the exclusive option for financial transactions, users will be left with no alternative but to disseminate sensitive data points across digital payment intermediaries.

Similarly to data protection, cybersecurity risks are framed as potential technical issues, untangled from the political, institutional, trust-related questions that they raise. In the emerging digital payment industry, cybersecurity matters are assigned to a "public-private partnership [...] launched by the Commission with the participation of the industry" (EPRes2017). The goal of increasing cybersecurity translates, once again, into incentives for companies to develop and implement more advanced technologies; for example, with regard to authentication, the Commission stresses that payment service providers "should rely on the most secure authenticating factors", i.e. biometrics, "moving away, where possible, from transmittable elements (e.g. static passwords) and from older technologies and communication channels that are prone to attacks (e.g. SMS text messages)" (CommComm2020). Cybersecurity, therefore, becomes an industry within an industry, which further strengthens the role of private actors in determining design, affordances, and data protection standards of digital payment networks.

A proposed solution to these data protection and security risks is the promotion of consumer awareness, literacy, and education about the functioning of financial technologies. There is awareness that regulatory frameworks might not suffice to protect consumers from potential abuses of data. To avoid risks of manipulation leading, for instance, to "hyperconsumerism", and "misselling practices", consumers must be aware of how their personal data are used for profit maximisation. There is a need to:

raise consumer awareness as regards both the opportunities and the risks related to innovative uses of consumer data (such as the risk of hyperconsumerism or misselling practices) (EBARep2017).

While recognizing the vulnerability of consumers/users of digital payment applications, institutions shift the responsibility of protection from the legal framework to users themselves. In the analyzed policy agenda, the recognition of the consumer/user as an actor to be protected does not translate into regulatory measures; the policy, in fact, favors data-intensive business models without questioning their long-term harm on individual choices and social dynamics. The awareness of potential threats, in fact, merely motivates the need to re-educate the consumer to fit the ideal of the free and informed market player who can benefit from competition and innovation.

4.6 CRITIQUE

The analysis provided in this chapter highlights how, according to policymakers, the digitization of payments realizes, and at the same time threatens, the interests of consumers. The dominant image – the one that is coherent with the future imaginaries depicted in the analyzed documents – is, however, that of a consumer who is empowered by technological innovation and benefits from a competitive digital market. While the goal of protecting consumers falls into the background, the mission of institutions is that of facilitating competition and the uptake of new technologies, creating a regulatory environment that allows technology companies to penetrate the financial sector, first and foremost opening access to financial data.

The notion of user empowerment is grounded on the rhetoric – promoted by the private sector – that, through digital technologies, individuals can better themselves and their lives. Hence, the consumer/user plays a role as a market player that is interested in the development of a fertile market for financial technologies, for the sake of their own self-empowerment. This interpretation implies conceptualizing the consumer as a free and rational actor who can enjoy full autonomy in their economic decisions, and benefit from the opportunities provided by the tech industry. Also, it is based on

the assumption that further digitization and technological development is desirable and necessary.

In the reasoning underlying the policy agenda, specific technological features (speed, usability, seamless experience, personalization, etc.) and technologies (AI, big data analytics, biometrics, etc.) are assumed to correspond to what consumers desire and need when it comes to digital payments. In a nutshell, the interest of consumers is tightly tied to a notion of technological empowerment, which in turn is grounded on a very precise sociotechnical imaginary about the future of payment technologies – one which mirrors the characteristics of emergent business models in the industry and disregards important considerations of consumers/users' vulnerability vis-à-vis digital applications (see: Dieter & Tkacz, 2020).

The technologies that are painted as desirable or necessary in the evolution of digital payments are the same – according to data reported in the 2019 EBA "Report on the impact of fintech on payment institutions' and e-money institutions' business models" – which technology companies have been investing in and experimenting with the most in recent years (EBARep2019). In the 2021 EU Commission Consultation on a new Digital Finance strategy, the involvement of citizens in determining what is desirable for the future of digital payments is scarce if not completely absent; only 5 responses were from EU citizens, while 125 came from industry representatives (Commission, 2021, p.3). Hence, it can be affirmed that – notwithstanding the centrality of consumer interest as a rhetorical catalyst for change – consumers have had little to no role in the definition of what is deemed desirable and needed in terms of technological change.

Arguably, features such as speed, personalization and user-friendliness are far from being an obvious preference for users of payment services. Banks' customers, for instance, might appreciate their institutions based on matters of trust, loyalty, and familiarity; they might be reassured by prudent, accountable bureaucratic procedures for handling financial transactions. Crypto-asset users, on the other hand, prioritize confidentiality over usability; they value technological creativity and the possibility of avoiding marketing and financial surveillance. Therefore, the technologies that are here portrayed as desirable

seem to be the product of a rather partial view, reflecting particular economic interests and discursive strategies.

"Consumer associations fear that algorithms may discriminate against those who are less willing to share their data online" (EBARep2017). Close monitoring of users' financial history and credit trustworthiness can lead to financial exclusion and prevent financial mobility. "Non-transparent dynamic pricing techniques" and "personalised offers [that] encourage frivolous spending or hyperconsumerism" make it questionable whether the cost reductions generated through data analytics and automation "would be passed on to consumers" (EBARep2017). The dominant argument of consumer empowerment could then be turned around: the transformation of payment services into a data-intensive platform-based industry, may – rather than empowering them – make consumers more vulnerable, less informed, and less autonomous than the classical market player assumed in EU consumer law.

Another critical point is the monopolistic and ever-expanding tendencies of platform economies. The possibility to choose amongst a variety of services is often prevented by the winner-takes-all consequences of platform network effects, which are likely to leave users little chance of opting out of the mainstream dominant payment applications. Hence, the market-based assumptions that free competition will ultimately favor consumers may be far-fetched. The traditional neoliberal axiom on the efficiency of market competition is gainsaid by platform logics; "the competitive struggle amongst surveillance capitalists produces the compulsion toward totality" (Zuboff, 2019, p. 497). The payment data market is not an exception to the tendencies shown by platform economies in other domains of activities: network effects are likely to hamper competition, with bigger technological companies establishing hard-to-eradicate monopolies.

The documents recognize the need to "address conduct and competition risks" (CommReq2021); reference is made to the applicability of the Digital Market Act[145] – "most of the large technology companies which are currently offering financial services are likely to fall into the scope of the

145 Regulation (Eu) 2022/1925 Of The European Parliament and of The Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828.

proposal" (CommCons2021) – which specifically addresses issues deriving from excessive market power gained by dominant digital platforms. Yet, in the policy agenda, the business models and the economic paradigm of platformization is not questioned, and its unwanted externalities are not critically analyzed.

The banking sector is likely to undergo the same process that occurred in the telecommunications sector in the early 2010s, whereby two global mobile platforms, iOS and Android, became dominant players in the sector, transforming telecoms "from the mediators of commerce to what are often called the 'dumb pipes'"(Steinberg, 2019, p. 16). Similarly to national telecoms giants, banks are likely to fall into the background of the payment ecosystem, leaving customer relationships and "data ownership" to fintech companies providing digital services and mobile interfaces. The alternative is for banks to themselves become digital platforms capable of providing competitive user interfaces; this option would ensure a more decentralized market, but the evident obstacle remains that of interoperability, whereas a unifying payment service infrastructure should bound together all banks' payment applications.

The evident risk, looking at the telecoms example, is to end up with a "de facto global regime of standards and shared operating systems" (Steinberg, 2019, p. 16) delivered and con- trolled from elsewhere. The issues deriving from this shift in the governance of financial networks can hardly be overstated; they range from the geopolitical oddness of delegating powers to survey and censor financial transactions to large foreign technology providers, to more subtle, long-term effects on individuals' financial behavior (e.g., hyperconsumerism), shifts in privacy perceptions, and social norms around money.

In conclusion, the policy agenda portrays a vision of the future of digital payment infrastructures that – whilst being painted as inevitable and necessary – is informed by precise narratives of user technological empowerment, which in turn reflect the interests of technology companies entering and shaping this new industry. The image of the consumer that is mobilized in the policy agenda is tied to arguments that reinforce the desirability of that future. This fixation with digitization and innovation can, upon closer inspection, be read

as the intention to refurbish a declining service industry as a data industry, resorting to data commodification and AI to reinvigorate revenues.

As more and more service industries are transformed into immense infrastructures of data extraction, the desirability of platformization as the dominant organizational model needs to be questioned more thoroughly; market regulation must be informed by considerations of the impacts of platformization on geopolitical power balance, labor conditions and individual rights, to name but a few.[146] Yet, in the policy agenda, the negative externalities of platformization, as well as alternative sociotechnical imaginaries, remain in the background, not urgent enough to inform political and legal reform.

4.7 CONCLUSIONS

Through a qualitative analysis of official documents, this chapter has investigated how certain imaginaries about technology filter into policymaking, allowing or accelerating the transformation of payment infrastructures into the platform economy. One of the ways in which socio-technical imaginaries filter into policymaking is, it turns out, by informing an image of consumer interest which serves to justify measures for the realization of a desired future. By attributing to consumers the need, and desire, for particular technologies, and technological affordances, and portraying competition as the best way to ensure them, policymakers appeal to consumer interest to justify their policy choices.

The thesis of this chapter is that the policy agenda in question relies on a notion of technologically empowered consumers which is grounded on partially constructed sociotechnical imaginaries about the future of payment technologies, and conceals an important consideration of consumers/users' vulnerability vis-à-vis digital payment platforms/infrastructures.

The dominant image – the one that is coherent with the future imaginaries depicted in the analyzed documents – is that of a consumer who is empowered by technological innovation, and benefits from a competitive digital market.

---

146 See: Panel for the Future of Science and Technology (STOA) (2021), Online platforms: Economic and societal ef- fects, https://www.europarl.europa.eu/stoa/en/document/ EPRS_STU(2021)656336.

While the goal of protecting consumers falls into the background, the mission of institutions is that of facilitating competition, and the uptake of new technologies, creating a regulatory environment that allows technology companies to penetrate the financial sector, first and foremost opening access to financial data.

The image of the future digital payment infrastructure portrayed in the policy documents is problematic for two reasons. First, the technologies and technological affordances that are assumed to meet consumer interest mirror emergent business models and products offered by the industry. Second, the assumption that more competition leads to the availability of more and better services – central to the whole policy agenda – is flawed, as the platformization process that the digital payment industry is undergoing entails the same risks of monopolization, dominance from foreign companies, and consequent geopolitical imbalances that are occurring in other domains. The notion of technologically empowered users linked to this vision is, therefore, partial. The negative externalities of platformization, and their implications for individuals, must be given greater consideration when determining the desired future of digital payments. Policymakers should look at other digital industries to be better understand the risks entailed by the platformization of critical infrastructures, and open their imagination to alternative possible futures.

CHAPTER 5: DIGITAL GEOGRAPHIES OF POWER: THE SCALE OF DIGITAL MONEY INFRASTRUCTURES

5.1 INTRODUCTION

In a 2020 article on the future of money and the role of the public sector, the President of the European Central Bank (ECB), Christine Lagarde, wrote that the digitization of society and of the economy must be accompanied by the digitization of money (Lagarde, 2020). The landscape of digital money networks that are built or speculated about is, in fact, extremely variegated at present. Controlled by private technology providers or decentralized networks of individuals located sparsely across the globe, digital money infrastructures challenge the traditional connection between the state, money, and territory.

In the past decade, one of the bigger provocations to money as the domain of public institutions came from cryptocurrencies issued and transacted over permissionless, worldwide networks which function without the legitimization and coordination of a centralized authority and without connection to a place or a clearly defined community. More commonly used digital payment networks are increasingly organized as data infrastructures, following the incentive systems of data markets, largely controlled by technology companies and platforms (Ferrari, 2022). Technology companies seeking to capture financial data streams are not only entering the financial industry as payment intermediation services; they also become e-money issuers, backing digital currencies that are native to their ecosystem

(Prasad, 2021).[147] Imaginaries bundled under the term *metaverse* suggest that the circulation of value and assets in the digital realm will be "unlinked from the political and territorial structures of nationhood" (Swartz, 2020, p.150) and tied to digital platforms' own ecosystems and incentive structures (Weiner, 2022).

Against the background of a digital payment and digital currency industry that threatens to undermine institutions' ability to exercise their monetary power (Pistor, 2020), initiatives are being developed to build digital money infrastructures as a public utility, re-establishing a link between money and institutionally-defined places or communities. These initiatives understand the capacity of money to organize and define social relationships, and the need to advance socio-political considerations concerned with the public interest in the construction of crucial infrastructures. The goals, political views, and institutional underpinnings of such projects are, however, unclear: they vary in terms of scale, socio-political goals, and technological design.

This chapter is concerned with investigating the relationship between scale, socio-political goals, and the infrastructural/technological design of digital money infrastructures. In particular, we investigate the development of digital money infrastructures as a public utility, as an attempt to contrast the ongoing tendency of global digital platforms to merge with and take control of payment and money infrastructures. Through a series of in-depth interviews about three publicly funded digital currency projects at the regional, local, and community levels, we analyze the alternative discourses and imaginaries that see money as a critical digital infrastructure to be shielded from corporations.

The focus on digital payment infrastructures – proposed by this chapter, and also reflected by the initiatives of financial and political institutions all over the world – becomes necessary, as it urges us to reflect on the modes of exploitation of financial data from both private and public actors, and on the merging of payment networks with the platform economy (Langley &

147 This threat was evident in Facebook's announcement of issuing the Libra digital currency; Amazon Coins are available to purchase goods and services on Amazon's platform.

Layshon, 2020). Importantly, directing our gaze to the infrastructure leads us to pose several questions: first, about the embeddedness of socio-political goals into the design of the technologies which enable transaction flows; second, on the modes of collection and uses of data; third, on the interests of the actors that build and govern money infrastructures (governance); and fourth, on the physical and virtual geographies that such infrastructures trace. These questions – that are briefly explained and contextualized in Section 5.2 – constitute the analytical tools around which the findings of the interviews are systematized (Section 5.4).

In the Methodology section, section 5.3, we describe the three use cases and show how the four analytical tools are deployed in a transversal manner to study and compare them. After an exposition of the findings, section 5.5 provides insights into how socio-political goals, governance, data use, and scale relate to each other in the analyzed use cases. We find that the larger the digital infrastructure, the less visible the local socio-economic issues and priorities; blind to micro economic dynamics and social relationships, supranational digital infrastructures are marked by a technocratic approach which hides important political considerations from public scrutiny. Smaller-scale digital currency projects, instead, are meant to realize alternative economic models that respond with high granularity to the needs and values of different communities. However, the more they disconnect from territorial political institutions, the more they lack scalability, consistent resource investment, and durability. Section 5.6 draws the conclusions, advocating for further investigations into the places and scales of digital money infrastructures.

5.2 BUILDING DIGITAL MONEY INFRASTRUCTURES AS PUBLIC UTILITY: FOUR ANALYTICAL TOOLS

5.2.1 SOCIO-POLITICAL GOALS

Historically, money has had a central role in the affirmation and exertion of state power (Helleiner, 2003). It is the node at the intersection between the political and the economical; or better, it is the medium upon which public institutions act to maintain a separation between the two – that is, to safeguard stances of public policy from the purely quantitative calculation of capitalistic

logics (Polany, 1944).[148] Money, therefore, is not merely a neutral technology of quantification: it is a *sign* of the social ties that are the foundation of the *communitas* (Amato, 2016). Its institution depends on particular configurations of trust and power in a community; its introduction and circulation in the community have the material effect of abstracting social ties into symbolic, economic, and institutional relationships (Redaelli, 2016).

Several examples of community currencies demonstrate that money can be harnessed as a medium to strengthen social relations within a community, transforming capital production into social production (Marx, 1844). As a symbolic system based on trust, money – that is: the legitimized currencies, the recognized *signifier* of value – is the first thing that must be changed in order to change modes of production and the types of market that exist within the community (Nishibe, 2016).

When money circulates in a digital form, the digital infrastructures underpinning its creation and circulation become an essential object of analysis. Inspecting money through the lens of *infrastructure power*, Braun and Gabor (2020) induce us to better investigate the apparently solely technical and neutral functionality of the underlying technological underpinning. Intended both as material objects and as networks of relations, digital financial infrastructures are deeply political: their accessibility, geographical extensions, and conditions of use shape opportunities, outcomes, and affordances in individuals' lives and society at large. A critical approach to digital money infrastructures, therefore, starts from inquiring the intentions and stated socio-political goals that are embedded in their architecture.

---

148 In capitalist societies, money pertains to the legacy of both public institutions and of markets, and it organizes both public and private relationships (Hart, 1986). Hart describes this duality using the metaphor of the coin: one side of it, the "head", symbolizes state sovereignty; the other side, the "tails", symbolizes money's commodity function, its role of measuring value and acting as a "trusted token" (Muellerleile, 2021, p. 247) to enable exchanges of objects within society. According to Ingham, two mutually dependent but distinct forms of power shape the conditions for capitalism: private economic power, oriented toward the protection of property and profit-making, on the one hand; and coercive territorial power on the other (Ingham, p. 244). Money, as Polany explained (1944), is the node at the intersection between these two form of powers; it allows the political to become economic. In other words, it is the medium upon which public institutions can act to maintain a separation between the two, to safeguard stances of public policy from the purely quantitative calculation of capitalistic logics (Polany, 1944).

5.2.2 GOVERNANCE

Technology occupies a liminal space between 'ideas' and 'material' factors
(BERNARDS AND CAMPBELL-VERDUYN, 2019)

Control over financial flows is founded on the control over the databases and networks which allow information about money and identities to be stored and circulated. Hence, discussions about the governance of money are necessarily discussions about the governance of the technology underlying this information flow. How is the technology architecture distributing power? What is the role of public institutions, and what is the stake of private actors?

Financial infrastructures are composed of commercial and institutional relations, cables, digital networks, and devices built and controlled by multiple actors. Governance is here understood as the set of more or less coordinated dynamics of social ordering which govern such actors, their relations, and the material components through which they operate. As such, governance comprises institutional norms (regulation, public administration, standard-setting, etc.), but also social practices and activities of multiple stakeholders, including NGOs, technology companies, technology designers, and community members (Musiani and De Nardis, 2016).

The three digital currencies selected for this study are prime examples of how digital infrastructure can bring changes in society, by moving agency among institutional actors, enabling bottom-up forms of financial organization, or reinforcing the legacy of old, conservative institutions. We focus on the governance *of* infrastructures by questioning how each project comes into existence, who governs it, who proposes policy choices, and how such choices are reflected and enacted in technological design. Moreover, we address, for each project, questions of governance *through* infrastructure: the ways in which these money systems act on social orders, altering or preserving pre-existing configurations of power in both its geographical distribution and institutional crystallization.

5.2.3 DATA

Questions about the governance of money are becoming questions about the spaces and rhythm of transaction flows. These transaction flows, mediated through digital platforms' APIs, are essentially data flows organized through digital infrastructures.

The digitization of money provides opportunities for the material infrastructure underpinning financial transactions to fall within the reach of technology companies.[149] It is the specter of bigtech platforms' sovereignty (Pistor, 2020) that pushes governments to develop data infrastructures within their domain of agency. The digital euro is precisely a digital infrastructure the scope of which is to maintain the circulation of the euro under the direct control of European central banks. Financial data is, in fact, key to public institutions for multiple purposes. It is essential to law enforcement, tax administration, and fraud detention, and it is used by banks and insurers to optimally allocate risk. The administration of sanctions, financial censorship, anti-money laundering, and anti-terrorist financing policies rely on the digital prints left by financial movements. Moreover, public institutions – regional, municipal institutions, or informal communities – can harness data analytics and technological design to influence individuals' economic behaviors, in ways that respond to predefined socio-political goals (Cristofari, forthcoming).

While on one end of the spectrum the control of financial data flows can put sovereignty and political power into the hands of global technology companies, strengthening forms of technological colonialism, it can also enable perfect surveillance and law enforcement, dramatically increasing the power of governments to interfere with individuals' economic and private transactions (Ávila 2018).

If the governance of money infrastructures is brought closer to the communities they are meant to serve, can data be used in ways that fit the values and goals of such communities? If digital infrastructures are built to serve the public good, how can financial data be managed in ways that respond to that goal?

149 Control of monetary flows has become a priority of bigtech platforms willing to incorporate financial data within their ever-expanding data flows. Payments are, in fact, a network market that well fits the multi-sidedness form of digital platforms, and is keen on market concentration.

Starting from these questions, we inspect practices of data collection and use as they are revealing of the politics inscribed in digital infrastructures.

5.2.4 SCALE

Both money and data are vehicles through which power is deterritorialized, stripped away from political institutions to private actors, and from communities and places to global colonizers (de Goede, 2020). In the form of money and capital, power moves across countries and flows through global networks "of variable geometry and dematerialized geography" (Castells, 1996, p. 359). A similar form of deterritorialization and reconfiguration of power relationships is determined by the digitization of critical infrastructures. Digital technologies are simultaneously local and global, national and international (Bernards and Campbell-Verduyn, 2019); they connect geographically sparse "places" and create new virtual "localities", dividing and rebinding communities, redefining the shape and the importance of borders. Digital infrastructures, therefore, are becoming a locus of contestation and coexistence among institutional actors, local communities, and global technology platforms as they allow power to be exerted in the form of data control (Pistor, 2020).

When money becomes digital, the challenge is to reconnect increasingly de-territorialized and de-institutionalized infrastructures to the *places* they are meant to serve. Digitization re-defines the meaning of *place* and institutes localities without geographies. The concept of *scale* – as "the representation of any area, as produced and defined by social process, from the smallest unit, the body, to the largest, the universe" (LeFebvre, 1974, p. 90) – is the starting point for a much-needed reflection on digital currency, political power, and spatial dynamics. In this chapter, we deploy the concept of *scale* to refer not merely to the geographical dimensions and boundaries of a digital currency, but also to the conditions for inclusion and exclusion, which determine the reach and the scope of the currencies within and beyond territorial geographies.

The element of scale here is helpful to frame considerations about governance, socio-political agenda, and the technological architecture of financial infrastructures; by pointing the attention to the (virtual or physical) geographies and the communities in which money flows, it serves as a thinking tool to

criticize and imagine future possible configurations of money infrastructures in relation to the places they serve.

5.3 METHODOLOGY AND USE CASES DESCRIPTION

The methodology of this chapter consists of the administration of in-depth interviews with persons involved in the development and/or implementation of three European digital currency projects. We conducted a total of 11 interviews between March and May 2022. All projects are funded and supported by European institutions; namely, they are: 1) the digital euro, 2) the Barcelona social currency, Real Economy Currency (REC), and 3) Commoncoin.

The digital euro is a project, currently at the investigation phase, aimed at the issuance of digital tokens which would serve as a digital version of euro banknotes. The digital euro would be issued by the European Central Bank in coordination with national central banks in the euro area, and it would be accessible to all European citizens and firms; we focus on its use for retail payments (as opposed to wholesale payments), as a complement to physical cash.

The REC is a local digital currency created and managed by Novact (NGO) and the Barcelona City Council for the city of Barcelona. It is initially used to administer a form of universal basic income, and in the long run it is meant to create a local exchange system that is complementary to the euro, with the aim of strengthening associative networks. The complementary local currency is designed to facilitate the consumption of local goods and promote sustainable supply chains.

Commoncoin is an experimental currency developed as part of the Commonfare platform.[150] The latter is the main outcome of the Poverty Income and

150 The project is part of the EU Commission strategy on "Collective Awareness Platforms for Sustainability and Social Innovation" (CAPS), aimed at "designing and piloting online platforms creating awareness of sustainability problems and offering collaborative solutions based on networks (of people, of ideas, of sensors), enabling new forms of social innovation". Organized as a collective research project composed of various pilot experiments, Commonfare seeks to challenge dominant economic models, including bigtech platforms "à la Uber, Airbnb, etc.", and offer "participatory economic models for welfare provisioning" (Interviewee 14).

Employment News project, a Horizon 2020 Research and Innovation Action under the EU Commission's Collective Awareness Platforms for Sustainability and Social Innovation policy. It is meant to work as an alternative currency for financing cooperative production and anti-speculative processes of production – in particular cultural production. The cryptocurrency system Commoncoin[1] is comprised of a digital currency and the Social Wallet API, which both support the implementation of cooperative welfare practices within communities. The project delivers these tools as a backbone infrastructure, leaving groups and communities the possibility to implement the technology with the further definition of technical and governance features.

The fundamental differential factor between these projects is the *scale* at which they are meant to operate. Starting from this central concept, we analyze these use cases to reflect on the relationship between the scale of digital infrastructures, the socio-political goals that drive their construction, and their technological design (including data use and governance structure).

Name	Scale	Institutional underpinning	Purpose	Status	No. of interviews
Digital Euro	Europe	ECB National Central Banks	Retail	Under investigation	4
REC	Municipality	Novact (NGO), EU Commission, Barcelona City Council	Retail/welfare administration	Active	5
Commocoin	Community	EU Commission Commonfare	Community building	Dismissed	2

Table 2: Source: Use cases overview. Elaborated by the author.

5.4 FINDINGS

In this section we summarize the findings of the interviews. For each of the use cases we identify and report the interviewees' responses regarding: a) the stated socio-political goals which motivate the project; b) the architectural and design choices that make the digital infrastructure suitable to achieve those goals, including issues related to data collection and use, as well as

aspects relating to infrastructure governance (comprising both institutional and technological underpinning); and c) the *scale* at which the project is meant to operate.

Project	Stated goal	Data use	Governance	Scale
Digital Euro	Financial stability Competition with foreign CBDCs and stablecoins	No intended use of data	Publicly owned infrastructure; reliance on third party service providers for user interface	Regional/global All citizens
REC	Stimulate local and circular economy Stimulate sustainable consumption Welfare administration	Use of data to optimize achievement of social goals In-app gamification and incentive systems	Governance shared between NGO and City Council, with involvement of citizens and businesses	Neighborhoods/city Recipients of welfare; Citizens
Commocoin	Enable communities' economic self-organization	Open to each community to define possible uses of data	Global backbone; implementation open to community specifications	Global replication of small-scale initiatives. Geographically sparse community members

Table 3: Summary of main findings, Source: Elaborated by the author.

5.4.1 THE (STATED) SOCIO-POLITICAL GOALS OF DIGITAL MONEY INFRASTRUCTURES

Digital euro

The European Central Bank (ECB) is a Frankfurt-based institution competent for the monetary policy of the European Union. Its main tasks are to maintain price stability, supervise banks, and guarantee financial integrity in the euro area. In collaboration with Member States' central banks, the ECB is investigating the potential implementation of what is known as a digital euro, conceived and engineered to work as the digital version of euro banknotes. The reason for its adoption would mostly be to respond to the need to ensure a public alternative to private forms of money. As cash is disappearing, in fact, no central bank money circulates among users and is available as a means of payment. The money that circulates through our plastic cards and mobile devices is "private money", i.e., guaranteed by commercial banks. The function of the digital euro is therefore that of safeguarding the availability of public money in the digital economy.

The starting point is the concern that we and other central banks have with private market players taking a share of each run of money (Interviewee 4)

According to the interviewees, the creation of the digital euro serves the public interest in three main ways. Firstly, public intervention in money supply is deemed necessary as access to digital money is conceived as a fundamental right to be legally ensured. Digital identity and digital payment accounts are increasingly becoming necessary to access all kind of services and to purchases products at convenient prices; hence, it is crucial that all citizens, regardless of economic, physical or other types of limitations, are able to use a digital financial account. Profit-oriented financial institutions and private digital payment intermediaries can deny access to financial services based on credit risk assessments or privately imposed censorship regimes. Hence, public financial institutions must ensure that the transition to the digital economy does not result in financial exclusion or discrimination in access to financial services. Secondly, a publicly controlled digital currency can be essential for the protection of privacy in digital transactions. A digital euro would in fact represent for citizens a viable alternative to commercial payment services whose

business model is based on personal data exploitation.[151] Finally, allowing a balance between private and public money supply (especially once physical cash disappears), the digital euro could be essential to safeguard financial and monetary stability. Central bank money is, in fact, a necessary backup and a last-resort source of stability when the private financial sector goes bankrupt (as happened in the 2008 financial crisis).

The above are the "explicit" motivations that the ECB would appeal to when justifying investments in the digital euro project before the public. There are, however, other less explicit but nonetheless pressing reasons for the initiative. It is, according to the interviewees, commonly understood within their institution that the push to initiate the digital euro investigation phase came after Facebook's announcement of its intention to issue a proprietary digital currency, Libra. Hence, it was the need to prepare for competition against global *stablecoins*,[152] or foreign CBDCs such as the digital dollar and the digital yeun, that forced the EU institutions to take action.

REC

Moving away from the European dimension, we zoom in on the city of Barcelona and investigate the political project behind the REC digital currency. The REC is a "social currency" developed by a private, no-profit organization (Novact) in collaboration with Barcelona City Council. Intended to work as a municipal complementary currency,[153] the REC has been initially used for the administration of welfare policies; namely, it has been used for the provision of universal basic income to Barcelona citizens. The provision of economic benefits via the REC served as a way to inject the currency into circulation.

---

151 On the commercial uses of financial data from private financial intermediaries, and its legal implications, see: Ferrari, V. (2020). Crosshatching Privacy: Financial Intermediaries' Data Practices Between Law Enforcement and Data Economy. European Data Protection Law Review, 6(4), 522-535.

152 *Stablecoins* are virtual currencies, the value of which is asset-backed (in physical collateral or crypto-assets) or algorithmically controlled in order to avoid price fluctuations typical of non-fiat digital currencies.

153 See: Doria & Fantacci (2018). Evaluating complementary currencies: from the assessment of multiple social qualities to the discovery of a unique monetary sociality. Quality and Quantity. 52. 1-24. 10.1007/s11135-017-0520-9.

The members of the REC project involved in our study (working for the NGO and the City Council) see money as a fundamental, non-neutral component of economic policies. The REC does not qualify as currency in legal or economic terms; it is a virtual alternative currency fully backed by (and at any time exchangeable with) the euro, and it is put into circulation as credit against local businesses. It can also be thought as a payment system in which euros are "tainted", bound to circulate within a small-scale local network of actors which includes citizens and local businesses.

The core idea of the digital currency is that of creating a financial system that better responds to the needs of the community in which it circulates; by promoting sustainable consumption and the circular economy, it wants to offer an alternative to capitalistic, globalized production and consumption models which strip wealth away from local communities and concentrate it in the hands of a few powerful corporations. The REC system encourages purchases from local producers and small retailers by embedding economic incentives into the design of the payment infrastructure, and by enabling expenditure of the currency in certain businesses rather than others; moreover, sustainable choices and solidarity among community members are valorized in non-monetary terms, through "rewards" in the form of digital tokens (NFTs).

> *A local currency is an incentive to buy the local product.* […] *In this way, it supports the development of the local economy. Because it changes, it generates resources for the local actors. And that improves their specialization* (Interviewee 6)

The flourishing of local economic activities also has the indirect effect of promoting physical social connections, generating social capital in the territory and strengthening urban inclusion. In fact, multinational supply chains also disperse expertise, as they move the purchasing of specialized production outside of the territory.

Commoncoin

A different socio-political project underlies the design of Commoncoin, the digital currency for the Commonfare platform. Commonfare is a EU-funded

Horizon 2020 project active in Italy, the Netherlands and Croatia, which develops along four main objectives: the establishment of a universal basic income; the bottom-up management of common goods and of the Commons; the development of an alternative ecosystem of production and cooperation; and the creation of a digital currency "for the Commons".[154]

The digital currency Commoncoin is a core component of the Commonfare research agenda. An alternative digital currency, Commoncoin is conceived as a provocative tool developed to provide a complementary, secondary line of credit to compensate for the euro system's inability to support people's basic needs. The intention is not to "replace" the institutional underpinning of credit supply, but to complement it, in order to compensate existing shortcomings in terms of welfare provision and solidarity. Essentially, Commoncoin represents a practice of resistance and a counter-imaginary to mainstream financial ecosystems.

The provocation and challenge was to try to apply participatory economic models for welfare provision (Interviewee 11)

Commoncoin is a digital currency that runs and is governed through the Commonfare platform, and is used by members of the Commonfare pilot projects: "Commoncoin is essentially the currency for the Commonfare platform" (Interviewee 14). The idea behind the Commoncoin currency is that of combining the principle of bottom-up organization and open-source culture with decentralized technological design, in order to enable communities' economic and social self-organization. While the backbone technological infrastructure is developed by the Commonfare project, the idea is that the single communities which adopt the currency can tailor its functioning to their own needs and goals. The digital interface and the terms and conditions of value exchange can, in fact, be modeled according to communities' needs and priorities.[155]

154 https://commonfare.net/it/pages/about

155 The pilot projects differ in objectives as they are tied to different groups, and the exact goal of the currency depends on the context in which it is implemented. Developers of the Commonfare platform ideally sit with "pilot communities" to study ethnographically the requirements of the technological infrastructure. The experimentation phase of Commoncoin developed through three main pilot projects: Macao (Milan) and Santarcangelo Festival in Italy, and Treehouse in Amsterdam, in the Netherlands. In Amsterdam, the pilot project was initiated by the Municipality to support the cultural and artistic sector; in Italy it has been experimented in the context of independent art festivals and organizations. In all three cases, the digital currency allows local communities to provide incentives for artists, in the form of a basic income of financial support for cultural events.

Money is nothing but the possibility to do [something]. It is the enabler of biopolitical production (Interviewee 11).

The ideological background behind Commoncoin is that money is a fundamental enabler of biopolitical production; instead of being put at the service of capitalistic logics of accumulation, it should be treated as a common good whose purpose is to "enable" people, opening possibilities for individual and collective flourishing. In line with the logics of complementary currencies, the proponents of Commoncoin support the idea that an ecosystem of currencies would provide more stability and granularity in responding to societal need, compared to the current monopoly of fiat money.

5.4.2 GOVERNANCE OF DIGITAL MONEY INFRASTRUCTURES

Digital euro

From an institutional point of view, the digital euro falls within the scope of the European System of Central Banks. The ECB, as the institution leading the investigation phase of the project, has established a High-Level Task Force dedicated to the project, involving representatives from national central banks. The Financial Stability Committee (FSC) and other subgroups of the European Commission also take part in the discussions.

The distribution of governance powers among the ECB and national central banks is an important issue still to be resolved; it is a crucial political decision, which will impact technological design choices in the construction of the digital euro infrastructure. One possible scenario is the use of Distributed Ledger Technologies (DLTs) to create a system of shared governance among central banks in the euro area. This would be a permissioned ledger where central banks would be controlling nodes. It is still unclear, however, whether a unified network will run throughout the eurozone under the supervision of the ECB, or whether the digital euro infrastructure will consist of a federation of national CBDCs directly managed by respective central banks:

This CBDC can link to national central banks, and then every country has its own CBDC. We can have CBDC NL, CBDC France, CBDC Belgium. […] *Or it could be the ECB running the CBDC.* (Interviewee 3)

In any case, it is unlikely that the architecture managed by central banks will include the interfaces (front-end software) through which citizens can access and transact the digital euro. According to the interviewees, central banks are not well equipped for (or willing to invest in) the delivery of "friendly" user interfaces and mobile apps. The issue is still the object of an ongoing discussion within the digital euro project, but it is expected that the digital euro will be stored and circulated through third-party service providers. This would imply involving mobile payment service providers – including U.S.-based companies such as Google Pay, Apple Pay, and PayPal – in the digital euro payment infrastructure.

Discussions are also open about the governance of Central Bank Digital Currencies at the global level. According to the interviewees, there are dialogues at the international level about how to manage the coordination (and competition) of CBDCs. The body that would take care of such coordination is the Bank of International Settlement, which would act as a global platform linking international CBDCs and enabling international payments.

> *If you have a euro platform and a dollar platform,* […] *then you can actually link the tool and you would also facilitate international payments.* […] *and if you have a platform approach, the whole thing becomes easier.* (Interviewee 2)

REC

Like every community project that wants to break ties with established institutional channels of power and funding, the REC project struggles to find a balance between the necessary level of institutional support and organizational and financial autonomy.

80% of funding for the REC comes from a European grant, and the remaining 20% from Barcelona City Council. The City Council has no ownership of the infrastructure, which is mostly developed and governed by the Barcelona-based NGO Novact. Nevertheless, the City Council has supervisory and decision-making powers regarding the scope and terms of implementation of the project, i.e., the duration, the neighborhoods in which it circulates, the businesses where it can be spent, etc.

We believe in this REC system being like a citizen currency. […] *It's not a property, it's not owned by the government. But we do need the support of the City Council.* (Interviewee 9)

The involvement of the City Council has, according to the interviewees, both advantages and disadvantages. The connection with Barcelona's public administration is fundamental for putting the currency into circulation. The REC is in fact "injected" as part of minimum income[156] to underwaged citizens in Barcelona. While this allows the distribution of the REC, it also implies that the adoption and use of the currency is in practice forced upon economically disadvantaged groups; its use becomes associated with less wealthy groups and neighborhoods, creating risks of discrimination for those who use it. Moreover, this scheme results in the paradox of pushing REC's societal and environmental goals on disadvantaged families.

The support of institutions makes the projects vulnerable to changes in power, and subject to slow, bureaucratic processes which hamper the success of the technological implementation. The members of Novact denounce the lack of consistent commitment from municipal institutions: as the REC does not bring direct economic growth, it has been treated by political powers as a temporary social experiment, with the termination of funding after a two-year pilot phase. While supported by Barcelona City Council's "Social Rights, Global Justice, Feminism and LGBTI" administrative area, the project is not supported by the Socialist Party in charge of economic policies. This has led to discontinuity in the development and use of the currency, and lack of financial support for its functioning. Proponents of the currency therefore advocate the need for the REC to be self-sustainable and independent from the political will of the City Council. According to them,

The negative side is that […when] *there are changes in power* […] *suddenly it can be situations in which the political support is not the same* (Interviewee 6)

---

156 The REC complemented the B-MINCOME project, a project aimed at "combining guaranteed minimum income and active social policies in deprived urban areas" https://uia-initiative.eu/en/uia-cities/barcelona. Under this project, 25% of minimum income was assigned to the recipient in RECs rather than euros, through the dedicated mobile application created by Novact.

The development and control of the technological layers upon which the REC currency is built and transacted is completely "in-house" at Novact for both practical and ideological reasons. Relying on third parties such as bigtech platforms for the provision of the app or cloud services would contradict the goal of the project of re-localizing the economy, and the flows of capital and data.

Practically, building and maintaining the system locally means retaining the ability to shape the technology based on the needs and priorities set by the project. This includes determining the conditions and the scope of data collection and analysis, and the use of information in line with the social goals that the local currency wants to achieve. Maintaining control and ownership over the technology is considered a fundamental requisite for the success of the project; hence, the technologies are not outsourced, even if this choice implies higher resource expenditure and the provision of slower, less efficient services and user experiences compared to mainstream digital services.

I think that it's really important to have your own technology so you don't rely on others for it. […] *And this is something that we can share, we can replicate, we can improve, and it's ours and we don't depend on others. Or at least we don't depend on big companies – that would be a problem.* (Interviewee 7)

Another important aspect in the governance of the REC is the involvement of the social actors that are directly interested in the program. The members of Novact, in fact, work in close collaboration with shop owners and citizens, garnering their opinions, and understanding their practices in order to tailor the workings of the REC to local realities at the neighborhood level. One of the future goals is that of creating a stable "Association of Merchants", a body involving local businesses in the co-creation and co-administration of the REC infrastructure, together with Novact and the City Council.

A very strong component is trying to involve local actors in the design of the currency; in the development of it. [We are]*trying to get them involved in supporting it and also in making the best of it.*
(Interviewee 6)

Commoncoin

The developers of Commoncoin share the view that open-source software and decentralized architectures can be used to bring *sovereignty*, decision-making and oversight powers to the people. Proponents of the Commonfare platform talk about the need to use subversive, bottom-up technological systems in order to "break technocracy" (Interviewee 10), so bringing the governance of the technology closer to those who are served by it.

> *I think that nowadays institutions are technocratic in their own soul* […] *to create technologies of liberation means to create technologies that release the power from the technocrats and give that to the people.* (Interviewee 10)

Therefore, transparency, auditability of code, legibility of coding language, open-source standards and principles are fundamental features of the platform's technological design.

> *To bring it closer to the people we need, on one side, to use free and open source and intelligible technologies,* […] *and then, on the other side, to facilitate a democratic process around decisions* (Interviewee 10)

The interviewees did not go into details about the technical choices that would materialize the proposed ideals of legibility, transparency, and self-organization. The backbone infrastructure of Commoncoin is based on blockchain technology; the Commonfare platform also provides the Social Wallet API for the storage and circulation of Commoncoin – a digital wallet which can be plugged into the applications built by the individual communities. By building second layer applications on top of the backbone blockchain infrastructure, communities can construct their own governance structure, voting mechanisms, and systems of value exchange.

5.4.3 DIGITAL MONEY INFRASTRUCTURES AND DATA USE

Digital euro

According to the interviewed experts on the digital euro, privacy is fundamental to ensure citizens trust a Central Bank Digital Currency; hence, the

infrastructure needs to be built with the highest possible level of privacy protection, i.e., as much confidentiality in the recording of transactions as allowed by anti-money laundering (AML) regulation.

The discussion around the technological design of the digital euro has mostly revolved around the possibility of using blockchain to build self-sovereign technological solutions[157] and allow anonymous transactions. However, this is prevented by AML rules, which demand that digital transactions beyond a certain amount are linked to individuals' legal identity.[158] The privacy issues and the threat of mass surveillance entailed by a digital payment network controlled by public institutions are so concerning that they, alone, might prevent the ECB from issuing the digital euro.

The issue of privacy will be very high up on the agenda of the ECB in deciding whether or not to proceed with issuing a central bank digital money, because it is possible that no solution that we will be able to come up with will meet a sufficient degree of approval. (Interviewee 4)

REC

As a socio-economic experiment, the REC project relies on data analysis to understand how the virtual social currency achieves the proposed objectives. The respondents specify that data is not used to observe and monitor individual behavior; rather, it is used at the aggregated level to get an overview of the changes in economic behavior at the aggregated level, to check whether the goals proposed by the project are met. In particular, data is collected to calculate the rate at which the REC stays in circulation within the local economy – i.e., the amount of RECs that are received from citizens by local businesses and reused by the latter to purchase more locally produced goods or services, instead of being exchanged for euros.

The idea is not to control citizens. […] *The only way we use the data is to analyze what happens with the flows of transactions, in aggregate* […] *For research*

157 See: Giannopoulou & Wang (2021).

158 This means that a digital euro would work on an "account-based system"; see: De Nederlandsche Bank, 2020.

purposes, it's very good to have all this data. But it's never used for anything else. (Interviewee 6)

The REC is meant to work not merely as a currency, but as a platform aimed at strengthening the community. Hence, it is organized as a "services environment" (Sergi), the main function of which is to connect and intermediate interactions among participants. The main "service" provided by the REC platform is information-sharing, which takes place at three levels: between shop owners, between shop owners and customers, and among the institutional actors involved in the governance of the currency. Moreover, this "service environment" includes added functionalities such as review systems for customers and maps locating the shops involved in the network (Sergi).

Like the proponents of the digital euro, the architects of the REC observe that citizens feel less threatened if data control is assigned to a private organization rather than to public administration; this justifies the leading role of the NGO Novact in the maintenance of the digital infrastructure and in the REC data governance:

Some people may be happier with the data belonging to somebody private, and not the city's government. (Interviewee 6)

Local digital currencies, functioning as an alternative currency to the euro, need to rely on various types of incentives for citizens to adopt and use the currency. These are either of a financial kind (e.g., receiving a bonus when exchanging euros for the local currency, discounts at local stores, or tax deductions for receiving wages in the local currency) or design-based. Gamification – the use of logics typical of games in contexts other than games[159] – is applied in the REC app to incentivize the use of the alternative currency, and to promote local and sustainable consumption. The interviewees talk about the use of NFTs, or digital tokens, as forms of non-monetary reward for citizens for participating in the project and contributing to its objectives.

---

159 On gamification, see: Ippolita, *Le tecnologie del Dominio*, Maltemi Editore, 2017, Milano, p. 107.

Commoncoin

The Commoncoin architecture is based on open-source decentralized technology – blockchain – that is, first of all, designed to guarantee transparency and trust in the governance and use of the digital tool. Data accessibility is therefore a central feature of the Commonfare platform and Commoncoin network. While users' identity and individual transactions remain pseudonymous for the developers of the backbone infrastructure, organizations and individual groups building on top of it can organize data collection, and use, according to community preferences.

The developers of Commoncoin are in favor of complete confidentiality and anonymity in the use of the platform: "My background is for strong privacy. […] And I think it should be completely anonymous, peer to peer" (Interviewee 11). However, they recognize the potential benefits of data analytics for policy choices, and for the technical organization of the incentive system. The project, in any case, stands against data monetization and any model that speculates on the use of data. Any possible use of data must be directed to the realization of the public good.

5.4.4 GEOGRAPHICAL DIMENSION AND SCALE

Digital euro

The digital euro is meant to work as a digital currency for the eurozone[160]. Within the eurozone, the primary goal is to make the digital euro accessible to all citizens, minimizing differences in access and usage among Member States. The investigators of the digital euro are aware of the huge differences among Member States, and between cities and countryside, in terms of digitalization and socio-economic types of relationships. The goals of uniform implementation of the digital euro within the European territory, and universal inclusion for the public digital currency, impose the need to deliver "user-friendly" technologies that can be used by people of all ages, regardless of their physical or mental state.

160 The union of the 19 EU Member States that have adopted the euro as their primary currency.

The whole economy is increasingly digital, and it is important for the public sector to make sure that nobody is left behind in this change (Weirts)

Yet, the dematerialization of the euro and its restructuring through digital infrastructures entail new possible geographies and conditions of access. The object of complex political and economic considerations are the conditions of access (the ability to hold digital euros) in non-European countries. It is confirmed by all interviewees that one of the aims of the digital euro is to "strengthen the international role of the euro" and to make the euro a global reserve currency. Hence, it is not excluded that non-European citizens will be able to open a digital euro account.

In terms of adoption, a balance needs to be found between the opposite eventualities of too wide an adoption on the one hand, and non-use on the other. The first would be at the expense of the private market for digital payments, undermining the interests of commercial banks. The non-adoption of the digital euro, conversely, would entail a loss of credibility and trustworthiness for the ECB.

If you introduce it and either it's not used or it fails, then there'll be a big problem for a central bank's credibility. (Interviewee 1)

REC

Conceptualized as a currency for the municipality, the REC is designed to circulate within communities of consumers and merchants that reside within confined geographical spaces. The system is developed in proximity with the population interested in its adoption: the developers of the REC observed networks of relationships and consumption habits in different neighborhoods in Barcelona to understand which actors would be most likely to adopt, and/or benefit the most from, the REC.

Based on assessments of existing local practices, the circulation of the REC is first of all encouraged at the neighborhood level, relying on social connections and familiarity among the residents. The idea is, in a nutshell, to encourage expenditure in small local enterprises rather than multinational retail shops such as H&M for clothing, or Lidl for food. In this manner, the REC

strengthens social cohesion within neighborhoods by consolidating networks of local businesses and incentivizing, through virtual rewards and financial advantages, consumers' loyalty to local shop owners.

In order to tailor the technology to specific social dynamics, paying attention to the specificities of single neighborhoods and parts of the city, the members of the REC projects conducted on-field dissemination and awareness activities. Education of the interested actors, and continuous communication with businesses and users of the REC, was deemed necessary for a proper integration of the app with the social practices of each place: "you need to really reach the people in the neighborhood" (Susana).

Our digital infrastructures want to complement and help physical relations, not substitute them […]*: our project is based on the streets, in the actual relations.* (Interviewee 5)

When it comes to expansion within the city, the priority is to attract "richer" neighborhoods and incentivize the use of the currency by wealthier people who could voluntarily support the REC's social and environmental goals. This is done, for example, by linking the REC to specific sectors such as the cultural industry or charity organizations.

We need to deploy the REC in some of the neighborhoods more involved in the social movement with very strong capacity to deploy this kind of money, […] *the hipster neighborhoods.* (Luis)

There is a vision of scaling up the adoption of the local currency to possibly include the entire city of Barcelona and even beyond, establishing connection with social currencies in other cities. Scaling up beyond the city level could happen in two ways. First, it could be done horizontally, through "replication" of the model in different cities, with crosspollination of projects and sharing of best practices – "the idea is to facilitate replication of the technology" (Susana) – and the practices around it in other local contexts. Second, it could be done vertically, through integration with the digital euro:

I see two ways of scaling up with this. There's replication, which is creating the same kind of thing elsewhere. […] *And the other […] idea is to work with Central Bank Digital Currencies in a way that they can back complementary currencies, local currencies like the REC.* (Interviewee 7)

Commoncoin

The vision of Commoncoin is that of creating a backbone-distributed infrastructure capable of scaling at the global level, untied from institutional powers and maintained through bottom-up organization. On top of such backbone infrastructure, applications can be built by communities, to create financial incentives or decision-making systems tailored to their specific requirements. The money infrastructure is therefore connected to community interest, but small scale does not mean geographical locality in this case. Commoncoin creates a locality without geography, recognizing that a community currency does not need to relate to a specific territory, or have a physical space as a connecting element.

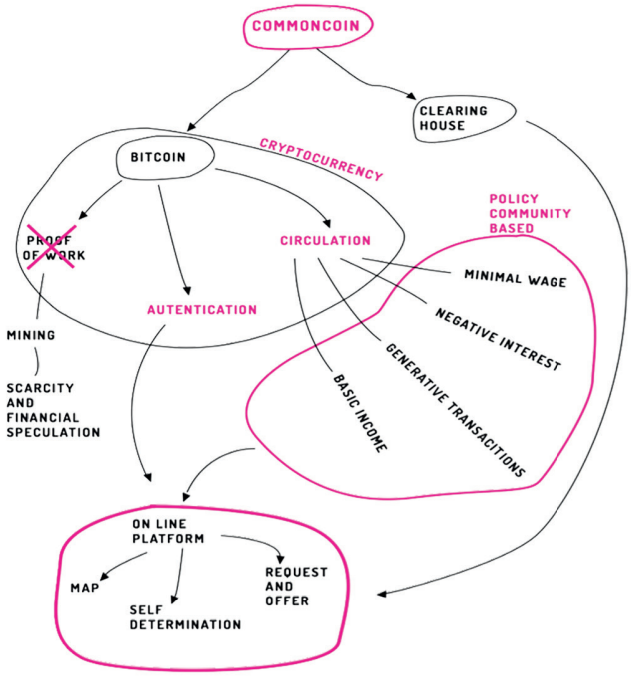

Fig. 7: Commoncoin, Macao project(Milan).

Global infrastructure but tailored to the local needs: the currency can work in the same way everywhere, but it has to be first managed at the node level in a geographically distributed way […] *in a way that local communities can still build their own rules* (Interviewee 11)

While the blockchain-based network would need to be able to scale in order to support multiple currencies running across the globe, there is a view that the single applications of Commoncoin should not reach wide adoption. Growth and expansion of one currency beyond the interest of the single communities would be against the premises of Commonfare; rather, the proliferation of independent projects and the evolution of a varied ecosystem of currencies is seen as the most sustainable solution.

5.5. CRITICAL EVALUATION

The three digital currency projects involved in this study share, as their underlying motivation, the core idea that money should be treated as a common good, and its functioning in society should be shielded from profit-oriented businesses.

The digital euro, the REC, and Commoncoin start from the premise that digital money infrastructures are a necessary component of digitized societies. The institutional, ideological, and political underpinnings of these three money infrastructures are different; yet, they all aim at ensuring people's right to access some form of digital economy.

The digital euro infrastructure is a large-scale financial ecosystem governed, in a top-down manner, by political and financial institutions that are competent in the governance of the euro and euro payment infrastructures. The digital euro project, led by the ECB, advances the idea that digital payments shall be provided as a form of Universal Basic Service: built and governed by public institutions, non-extractive, and available for all EU citizens. The service should be free at the point of use, and the digital architecture design should respond to the prerogatives of the *common good*, actualizing the right to a European digital citizenship.[161]

161 See: Muldoon, 2022, p. 21.

The ambition of *universal scaling* brings the digital euro away from the places and communities it is intended to serve; the narrative is that of a *neutral* digital infrastructure whose operations are not meant to alter current socio-economic practices and power balances. While it would allow a uniform, cross-national, coordinated implementation across the EU, it does not allow social and economic players to tailor the workings of digital money to local contexts. The supranational dimension of the digital infrastructure, and of the actors involved in its construction, mean less attention for national and local socio-economic issues. The geopolitical considerations that emerge in discussions regarding the digital euro do not relate to the internal geography but to the external, global network of "competing" National Digital Currencies or private stablecoins.

Delegated to highly technical bodies, the development of the digital euro takes place outside of public debate. The construction of the digital euro seems to be moved by the double goal of preserving the legacy of banks in the digital age on one side, and ensuring efficiency in digital payments on the other. Seen as something highly technical, the digital euro is designed in a top-down manner, without the involvement of citizens (van der Linde & Bollen, 2022) and without any ambition to address socio-economic issues. It ultimately perpetuates the status quo when it comes to the balancing of power between central and commercial banks, and between banks and technology businesses. Critically, in fact, it leaves a crucial part of the payment infrastructure, namely payment intermediation services which interface with users on mobile devices, to commercial digital platforms.

A different political agenda lies behind the experiment of the REC social currency. "Platform socialism starts at the local level": the proponents of the REC seem to ascribe to a form of what is called *new municipalism*, sustaining the idea that the municipality is a strategic site for giving power back to citizens (Muldoon, 2022: 101). The premise for the construction of a local digital infrastructure like the one underpinning the REC is that problems brought about by globalization must be addressed by refocusing on the local.

The REC challenges the status quo by trying to prove that digital infrastructures can be built and governed within the place they are meant to serve. Far from proposing blind faith in local political institutions, the REC

project seeks to restore democratic control over the local economy through public-common partnerships in the governance of the digital infrastructure. This model allows, on the one hand, the identification of local problems and solutions tailored to the needs of the local community. On the other, it ensures the involvement of a plurality of actors (public institutions, NGOs, civil society, and citizens) who can cooperate on the co-production of digital infrastructures, negotiating socio-political goals in a stable and durable manner, as long as institutional and financial support exist.

The REC project, however, demonstrates the risks, obstacles, and downfalls of this kind of pseudo-institutional digital activism. The ambition to emancipate the project from the (unstable) support of local political institutions risks leading to forms of *entrepreneurial activism* (Muldoon, 2022), where sources of revenue for the continuation of the projects must be obtained from users, through fees, advertising, or data monetization. This would imply a departure from the *public utility* model that the project is meant to actualize. Moreover, the local social currency encounters scalability issues that seem to be hard to circumvent. The small-scale dimension of the project within the city translates into an uneven demographic of the currency user base, with possible consequences in terms of discrimination and biases toward users if the use of the currency becomes an indication of their *social status*. Moreover, the lack of network effects ensuring high circulation of the currency threatens to undermine its usability, even in the local realities it is meant to serve.

The Commoncoin experiment, finally, represents a departure from *social democratic* approaches of building digital infrastructures as public utilities supported by administrative public institutions. The project, in fact, promotes an agenda that goes against centralized power and decision-making. The underlying vision is that bottom-up economic organization, participatory planning, and collaborative culture are necessary for democracy and freedom. The value of this project is that of offering a counter-imaginary that rips established powers away from their hegemony of the construction of digital infrastructures. It is aimed at enabling resistance practices scattered beyond geographical boundaries, overcoming the pre-established institutional boundaries that organize financial flows and economic exchange.

None of the Commoncoin pilot projects, however, have resulted in a durable solution; the Commonfare platform did not realize any successful application with a relevant scale of adoption in the field of digital currency creation. Notwithstanding the value of Commoncoin as imaginative resistance practice (van de Donk et al., 2004), it must be acknowledged that the ambition of leaving communities the task of building and running their own applications did not result in concrete, bottom-up initiatives. This highlights the struggle of building and maintaining digital infrastructures in a bottom-up manner, and suggests that durable digital infrastructures require resources, expertise, and lasting political commitment, which are difficult to maintain without some form of institutional underpinning.

5.6 CONCLUSIONS

Confronting the use cases selected for this study highlights how digital infrastructures have become the locus of contestation between commercial actors, institutional powers, and communities. If reclaimed from tech corporations and built as public utilities, digital infrastructures can be shaped by institutional political agendas imposed from above, or serve as tools that give agency to bottom-up organizations and political activism.

The three initiatives – the digital euro, the REC and the Commoncoin – differ in terms of scale, not only territorially, but also as virtual spaces determined by conditions of access and inclusion. The observed projects seek to build payment/money infrastructures in connection with different geographical or digital *localities*; such localities are identified on the basis of political/economic considerations, and their identification translates into particular configurations of the technical underpinning of the digital infrastructure itself. The analysis and comparison of the three use cases, therefore, offers some reflections, and allows some conclusions to be drawn about the relationship between the socio-political goals that are ascribed to money infrastructures, the governance, and technical design of such infrastructures, and the scale at which they are meant to operate.

Regarding the relationship between scale and political purpose, it can be observed that if the scale of the digital infrastructure becomes larger (i.e. in our case, regional, EU-wide level), the socio-political purposes that are

inscribed in such infrastructure become less granular. In other words, the larger the digital infrastructure, the less visible the local socio-economic issues and priorities. The digital euro, meant to work at the regional level under the direct control of European financial institutions, does not direct its gaze to local socio-political issues; it is blind to micro-economic dynamics and social relationships, and proposes a rather technocratic approach that sees the digital infrastructure as a neutral, highly technical matter to be managed by institutions in a top-down manner. This translates into a governance model centralized around competent institutions and financial actors that are loosely connected to territory; data collection is minimized or outsourced, whereas cooperation with private technology providers is maintained for the provision of mobile payment applications and user interfaces.

On the other hand, municipal initiatives build their digital infrastructure with attention for local economic issues, and seek to maintain technological governance within the agency of local actors and citizens' oversight. By relying on cooperation between civil society through local NGOs and public institutions, the initiative at the municipal level is potentially able to deliver a durable, digital infrastructure that responds to citizens' needs, and is tailored to local businesses' dynamics and issues. At the city level, a plurality of actors (public institutions, NGOs, local businesses, and citizens) can cooperate in a stable manner to build and control digital infrastructures, negotiating the socio-political goals to be inscribed in it. Through this synergy between different stakeholders, the municipal level becomes a strategic site for reconnecting civic society and the governance of digital infrastructures.

While the municipal currency REC identifies the city of Barcelona – hence a geographically and politically identified space – as its *locality*, the Commoncoin project sets up an infrastructure for *digital localities* that are not defined by territory or political institutions. The Commoncoin project seeks to enable more strictly bottom-up models, enabling self-identified communities to autonomously specify, implement, and govern their own applications for value circulation. This would ideally underpin alternative economic models and technological systems that respond with high granularity to the needs and values of different communities. However, the experiment has not resulted in successful implementations, suggesting that non-institutionally

defined communities lack the resources and governance structure to create and maintain long-lasting and usable digital infrastructures.

We found the issue of scale to be central in discussions about digital money infrastructures, as the concept highlights the interconnection between territory, political institutions attached to that territory, and infrastructures. It also directs focus to the tension between increasingly global digital infrastructures and the localities they are meant to serve. The list of questions, tensions, and challenges is, however, long: multiple lenses should be deployed in tandem to better determine the possible paths for reconnecting digital infrastructures with people and places. Hence, we conclude by advocating the need to further question the place, scale, and political goals of emerging digital money infrastructures.

CHAPTER 6: GENERAL CONCLUSIONS. IMAGINING SOMETHING ELSE: IMPERFECTION, PLURALITY, RE-LOCALIZED AGENCY

Groups are made, agencies are explored, and objects play a role. Such are the three first sources of uncertainty we rely on if we want to follow the social fluid through its ever changing and provisional shapes.

BRUNO LATOUR, *Reassembling the social*

Digital value transfer infrastructures can take many shapes; whether they are centralized around one single center of command, decentralized across geographically sparse computer nodes, scalar, or fragmented like a rhizome, they draw particular power configurations and trace certain geographies of political spaces.

Payment functionalities embedded in commercial platforms' ecosystems, digital tokens circulating over distributed peer-to-peer networks, central bank digital currencies, and local or community digital currencies are all examples of socio-technical assemblages that seek to organize economic and social interactions through systems of value representation and circulation. Each of these systems of value flow is, in turn, the materialization of particular socio-technical imaginaries as produced by different social, economic, and legal institutions.

Throughout the chapters of this book, I have analyzed different digital infrastructures of value flow, picking them from the reality of the multiple initiatives that are taking place at the time of writing. Using different

methodological approaches, I have unpacked their material and social construction, assessing the societal functions they propose to fulfill. I have retraced the motives and the mechanics that drive their development, to test them against the logics and the mechanics of another equally complex, yet somehow more predictable system: the law.

The various questions posed when studying these cases – privacy, law enforcement, socio-technical imaginaries guiding policymaking, scales of institutional organization – are all, in different ways, addressing the central problem of how the development of digital value transfer infrastructures is influenced by, and contributes to, processes of legal change and redistribution of power across various geographies.

Telling users apart: the imperative of transparency and the limitations of the legal construction of privacy

The first issue that requires inquiry when addressing the digitization of value transfer infrastructures is the erosion of spaces for confidential, untraced transactions. This issue has been dealt with in Chapter 2, which explores privacy issues in financial information networks.

The digitization of monetary flows allows information about financial activities to be gathered, traced, and contextualized with previously inconceivable levels of accuracy. Demands for transparency following 9/11 on one side, and the 2008 financial crisis on the other, promoted a culture of surveillance expressed first of all as increased oversight of monetary flows. Practices of financial monitoring are situated more broadly within a trend of securitization that involve forms of actuarial justice and risk-based, algorithmic regulation (Amoore & de Goede, 2021; de Goede 2020; Yeung, 2018); these involve processes of individual and group profiling through data analysis, and automated categorization and decision-making (Hildebrandt, 2009).

The fintech domain – where technology and finance converge – is dominated by the mantra of transparency and efficiency; efficient information management is aimed at the reduction of human arbitrariness in auditing and decision-making. Information and automation, meant to avoid mistakes and inaccuracies in the detection of "unusual" behaviors, are thought of as

conditions for economic optimization. All processes, taking place as information circulation, must be informed by speed and measurability. Information infrastructures must be free of "gaps" and blind spots. [162]

The overarching ideals of efficiency and transparency translate into ambitions of *perfect enforcement* and *perfect targeting* that insert individuals into numerous data-driven technologies. Financial information crosslinked with social media and demographic data informs profiling for law enforcement and commercial purposes. Individuals can be granted or denied loans, offered tailored financial products, or inserted into *risk* categories[163] based on algorithmic assessments. For these reasons, the fintech domain is also full of examples of how technologies of datafication and automation bring about risks of discrimination toward individuals who deviate from the normative majority (Guyan, 2022).[164]

The dominance of *transparency* in the public discourse in general (Han, 2015), and in the fintech domain in particular (Herian, 2019), – predominantly invoked in connection to corruption, and threats of terrorism – risks paving the way for a *post-privacy* culture in which the private sphere is sacrificed in the name of see-through, operational, controllable, readily available information.

Increased digitization and liberalization also insert new actors, and new logics, into the functioning of the value transfer infrastructures. Mobile banking and mobile payment services enter the scene to fit the "modern, mobile lifestyle

---

162 Some scholars have questioned the belief that more information leads to better readability and better decisions, arguing that such a belief is grounded on the naïve, mistaken idea that human lives are readable, predictable, and comparable. As Han points out, "human existence is not transparent, even to itself" (Han, 2015, p. 3). Excessive, humanly unreadable information mediated by ubiquitous and concealed technological infrastructures has been proven to undermine, rather than enlighten, our understanding of individual and public life (Hong, 2020, p. 49).

163 For example, in the context of Financial Information-Sharing Partnerships among private actors and law enforcement bodies, individuals can be tagged as *persons of interest* prior to being suspects in criminal investigations. No clarity exists on what criteria are used for such a determination, and individuals are not informed about their personal data – including their financial networks – being shared and analyzed in the context of investigations.

164 "Transparency stabilizes and speeds the system by eliminating the Other and the Alien. This systemic compulsion makes the society of transparency a calibrated society. Herein lies its totalitarian trait" (Han, 2015 p.2).

of today's customers".[165] With technology companies penetrating financial information networks, financial data enters the data economy. Data collection and analysis is aimed at profit maximization, involving personalized marketing, behavioral nudging, and expansion of data points with crosslinks to social media information.

As discussed in Chapter 2, the linking of financial data with broader sets of data points involved in commercial data practices calls for increased privacy protection in the form of, first of all, GDPR enforcement. However, law enforcement prerogatives, demanding systematic collection, data retention and oversight, compress the applicability of the GDPR and the enforceability of the rights enshrined therein.

In the EU, privacy and data protection are both enshrined as fundamental individual rights to be shielded against the interests of private commercial players involved with practices of data extraction and exploitation.[166] The GDPR grants various rights to individuals to interfere with and determine the use of their personal data by companies. But in an apparatus where identification and authentication are perpetually re-assessed, transactions' sources and destinations compulsorily verified, and identifiers never erased, the activation of privacy protections at the level of individual users is a weak counterbalance.

Digital information infrastructures can reach levels of ubiquity that allow detailed monitoring and oversight of individuals' activities and movements. The actors that participate in such infrastructures by recording, organizing, and retaining information are in powerful positions: they can oversee as well as influence and engineer human actions and relations. Containing such power would imply – as the GDPR itself suggests[167] – imposing data protection and privacy not only as legal norms, but also as principles of technological

---

165 Private Equity Forum (2018). 'Brief insights from PEF research. N26: the rise of a fintech'.

166 Fundamental rights are, in fact, increasingly invoked beyond their traditional field of application, which sees them as legal devices against state power; they are increasingly becoming regulatory imperatives binding private companies which hold positions of power as gatekeepers in multiple domains of activity. The GDPR is seen as a prime example of this broader trend.

167 Cavoukian A., 2009.

design determining the material underpinning of digital communication and transactions.

In my conclusion of Chapter 2, I have suggested that the coexistence of law enforcement prerogatives and privacy as legitimate legal interests requires admitting spaces where one is sacrificed for the benefit of the other. In the landscape of initiatives aimed at developing value transfer digital architectures, regulators should allow, or even encourage and contribute to the construction of, privacy-preserving means for digital payment. To counteract the risks of a financial industry that buys into the logics of surveillance capitalism, research efforts and political commitment are needed in order to safeguard, or build, spaces for confidential transactions.

Codifying objects, licensing actors: legal entropy and the problem of the "outside"

Infrastructures circulating media of value that economists would refer to as money in the proper sense are information networks institutionalized and standardized by sovereign states. Such infrastructures are born with, remain intrinsically linked to, and are fundamental to the exercise of political authority that is first of all a threat of violence against financial default (Graeber, 2011). Public administration, welfare and taxation policies, as well as law enforcement in general, largely depend on governments' ability to access information about monetary flows. The institutions, businesses, and technologies that mediate such flows are deeply intertwined with the exercise of state sovereignty, bound in a sort of "information mercantilism" (Rosenbach & Mansted, 2019) with law enforcement apparatuses.

Conversely, peer-to-peer, digitally native cryptocurrencies circulate over worldwide digital infrastructures built and maintained by geographically sparse groups of developers with no ties to law enforcement authorities. Decentralized cryptographic protocols for value circulation were first experimented with as privacy-preserving tools that could eventually be integrated with political and economic institutions (Chaum, 1985; Agre 1999). However, such integration did not take place. Cryptocurrencies' ecosystems conceive of themselves as architectures that escape appatuses of enforcement (May, 1992; Nakamoto, 2008). They developed as "an outside" (Fumagalli, 2016):

as hardly controllable, hardly detectable value transfer systems which, by de-linking payment addresses from users' identities, carve out those spaces for confidential transactions that efficiently policed financial infrastructures do not allow.

The competition between these two models has not only been played out over technological design and legal compliance; it has been, ultimately, a competition between different types of social institutions and ideals of political legitimization. Distributed technological systems ultimately propose a re-thinking of economic interactions, techno-political governance, identity management, and rules enforcement.

In the absence of stable forums where these two worlds could engage in institutional dialogue,[168] both sides – legal institutions on one side, blockchain communities on the other – reacted with complex, inconsistent strategies, sometimes integrating within each other, and sometimes reinforcing their mutual incompatibility.

Not recognizing any communication apart from legal communication (Luhman, 2004), the legal system tries to reconduct everything within its categories and schemes. The lack of integration of the fundamental premises of the token economy within dominant economic institutions made it such that, to be profitable in the real economy, these initiatives started to conform: they got licenses, worked within clear legal frameworks, and issued tokens that are substantial equivalents of conventional types of financial assets (the best example is the shift from so-called "Initial Coin Offerings" to "Security Token Offerings"). Part of the blockchain ecosystem renounced the original ideal of decentralization, and abandoned its open-source roots to transform itself into a highly intermediated market. A whole new range of intermediaries – from exchange platforms to custodian wallet providers – emerged, endorsing Know Your Customer and Anti-Money Laundering compliance schemes, demanding users' authentication to ensure business continuity.

---

168 Note that it is a necessity for these forums not to exist. Both states and blockchain communities preserve their "sovereignty" precisely because they do not recognize each other as valid interlocutors.

As exposed in Chapter 3, the development of the blockchain industry offers an interesting illustration of the impact that regulation has on the development of digital markets and their technological architectures. By incentivizing compliance, making it if not necessary at least convenient for any socio-technical endeavors to organize as legal, documented entities, regulation contributed to the re-centralization of the web around legally identified, economically productive market actors.

But the evolution of the cryptocurrencies' ecosystem continued in spaces that the legal system could not capture, with ever-changing types of tokens evading categorization – technological escamotages to circumvent liability schemes. The ecosystem kept growing, fundamentally impossible to ban, tax, or unplug. This impossibility derived from the fact that what the law tries to capture is not a static object; it is not a single subversive political movement or a fraudulent economic endeavor. It is a readily available, non-scarce and effectively enforceable tool for groups' self-organization: the continuous making, updating, and unmaking of digital infrastructures that express groups' political, economic, and institutional agency (Latour, 2005).

The legal system tolerates socio-technical phenomena which escape its categorization and mechanisms of enforcement as long as the latter do not fundamentally threaten to undermine its functioning.

When Facebook announced its intention to create its own cryptocurrency, Libra, which would have circulated through its platform, potentially becoming a "global currency and financial infrastructure that empowers billions of people,"[169] national jurisdictions understood the implied danger of losing some of their monetary and political power. Ultimately, what made Libra impossible was not a strong and clear incompatibility with legal rules,[170] but rather, an imaginary of systemic risk averted through the discretionary power of institutions. The legal system reacted based on a fundamentally political rationale: the fear of bigtech platforms' monopoly expanding into the financial domain.

---

169 Libra, white paper.

170 In fact, the Libra structure was more legally compliant than decentralized anonymous cryptocurrency networks like Bitcoin, yet it was the former that was strongly prohibited by U.S. and European institutions.

The worldwide platform, in fact, would have established a form of global dominance not only setting standards and directly governing financial infrastructures, and interfaces of value flows, but issuing and controlling the circulation of its own media of value. Facebook, by promising the use of blockchain technology, linked its project to the ideas of disintermediation, decentralization, and transparency. Yet, in reality, the techno-political project of establishing a platform currency was the ultimate step toward the configuration of a "platform-state", where the digital platform becomes a mediator, enabler, and architect of not only inter-personal but also institutional relations. Libra would have been the symbolic and functional materialization of an unprecedented corporate sovereignty, crystalizing the platform's autonomy in the exercise of political and economic power (Ferrari, 2020). But (supra-) national institutions (to be precise, the U.S. Congress and the European Commission) showed their teeth: the Libra was an example of an "outside" that was too big for the legal system to tolerate.[171]

By exploring the regulatory and technical enforcement challenges posed by blockchain-based crypto-assets, Chapter 3 has demonstrated that regulation plays an important role in directing the development of the technology: the practices it enables, its geography, and the extent of its adoption. In line with the argument made above, the findings of Chapter 3 suggest that the regulation of digital environments should be guided not only by the intention of preventing illicit activities, but by normative choices that determine what kind of economic models and institutions are given priority over others in the organization of public life.

While regulation determines the integration of social and economic practices within broader legal institutions, "outside" spaces develop with or without institutional endorsement. Without institutional integration, alternative socio-economic experiments such as crypto-currency ecosystems are doomed to remain a form of resistance, and a provocation to dominant models increasingly centered around extractive digital platforms.

---

171 See also: Ferrari V. (2020). Tecnologie e geografie di potere delle piattaforme digitali: Libra. Kabul Magazine.

Platformization and policymaking

> *The design problems require speculation but are not hypothetical. They demand that we engage a response that is as inventive as it is ineluctable.* (BRATTON, 2016, p.53)

Chapter 4 exposes the process of platformization that is pervading most areas of social and economic activities. This model is based on the centralization of contractual agreements, transactions, and relationships within and across markets around a single, tentacular entity. User authentication is one of the fundamental components of the network of dependencies that digital platforms establish around themselves, bundling people and services within their gated ecosystems.

The analysis of the policy agenda on fintech in Chapter 4 shows that European institutions have precise visions of what the future of digital money infrastructures should be, and this vision poses the platform model as an obvious organizing principle. The regulatory agenda pushes for models of fast, seamless, and ubiquitous authentication through mobile devices; payment interfaces need to be interoperable across services. To achieve these goals, they must be embedded in platforms' ecosystems.

Yet, platformization in adjacent areas of activity has raised several legal and political issues, leading to the adoption of regulation aimed at preventing unwanted consequences of this business and organizational model (such as the DSA and the DMA). Concerns are also voiced in the fintech agenda itself, including data protection and privacy considerations, unfair competition and abuse of market power, consumer protection, and more generally challenges to national sovereignty raised by globally dominant, non-EU-based bigtech platforms. Yet, these concerns are not strong enough to push regulators to challenge the *platform capitalism* (Srnicek, 2016) model altogether and imagine, let alone propose, something else.

The coexistence of a vision informed by the platform imaginary, and fears stemming from it, results in regulatory efforts that are in apparent contradiction with each other. On one side, the GDPR imposes data minimization and careful sharing agreements among companies and institutions; on the

other side, the PSD2 forces banks to open their databases to data-intensive technology businesses, favoring the expansion of the platform model.

However, the apparent inconsistencies between the legal frameworks are, upon closer inspection, not inconsistencies at all: their coexistence in the same system makes sense exactly because one is meant to temper the damages brought by the other. The GDPR is constructed on the premise that data are channeled by centralized, commercial digital services. It assumes that information stored in databases and flowing across digital networks is always relatable to identified and authenticated "data subjects"; it does not conceive absence of controllership; and it implies the existence of an easily identifiable responsible actor, an entity that "owns" the data and has the power to "give it back" to users upon demand (Giannopoulou & Ferrari, 2018). The legal institutions that are meant to "protect" users from the power of digital information gatekeepers are structured on the assumptions that such power remains in place.

The institutional promotion of the platform model reflects the neoliberal economic strategy guiding policymakers in the construction of digital infrastructures. Centralization – the argument goes – increases efficiency and reduces transaction costs; liberalization leads to cheaper, better, and faster technologies that can be offered to users at lower prices. Yet, the value produced by technology companies in the fintech sectors is extracted from the data produced by users' interaction with the system. "Embedded" finance encompasses payment intermediation, lending, insurance services, and credit risk assessment, de facto placing technology companies in the front line of the financial service industry.[172] Banks demand a whole range of documented information in order to grant a loan; these companies, conversely, possess so much information about users that they can predict (fabricate) users' needs and offer financial products before users even ask for them.

As highlighted in Chapter 4, the insistence on "efficiency" as a policy goal in the European fintech agenda signals the partial view that traps regulators' imagination. The data accumulation logics that drive platform capitalism, in fact, reduce the positive outcomes of "efficient" technologies. Ultimately, a

172 Irrera & Withers, 2021.

more efficient service for the consumer is a more efficient way of exploiting consumer data for the platform. For example, the time users save by using smoother, faster interfaces is lost in prolonged interactions with the digital ecosystem, as the latter is designed to smooth such interaction but also maximize the time users spend on the platform. When Amazon offers users the possibility to buy now and pay later, it lends money at an interest rate of zero, and ultimately increases its revenues with more purchases, gaining competitive advantage in the market and maximizing users' *data labor*. Users, on their side, will ultimately run the risk of hyperconsumerism and find it increasingly difficult to return to other modes of organizing their finances outside the platform.

As shown by the findings of the empirical analysis in Chapter 4, the European policy agenda on fintech relies on a notion of technologically empowered consumers which is grounded on partially constructed sociotechnical imaginaries about the future of payment technologies – a notion that conceal important considerations on consumers/users' vulnerability vis-à-vis digital payment platforms. The *empowered* subject envisioned by the European regulator is, indeed, benefiting from faster and smarter technologies; yet the real value is not the one that she perceives to be gaining, but the value that is produced through her very interaction with the extractive digital ecosystem (Van Doorn, 2014; Sadowski, 2019; Fuchs, 2021; Srnicek, 2016).

Regulatory efforts cannot overcome the power of platforms if they do not overcome the neoliberal discourse that sees platformization as an optimizing force and economically efficient model. The notion of technologically empowered users should be compensated by necessary reflections on the negative externalities of platformization. To this aim, imaginaries of something else – even if they have so far failed to materialize viable alternatives integrated with broader economic, social, legal institutions – are relevant, and should be taken seriously in processes of legal change.

New geometries and geographies of digital value transfer infrastructures

The institutionalization of value depends on social conventions, as much as on the materialization of the media that allow value's representation and circulation. When value is represented and circulates as digital media, the digital infrastructures that are necessary for such media to circulate become the frames of new architectures of power and vehicles of social agency.

Understanding the geographies traced by emerging digital value transfer infrastructures is crucial to delineate the dynamics of power that are decentralizing politics from nation-states and their institutions. Unpacking these dynamics is a challenging task, as they involve new actors and new material architectures through which power is institutionalized, and value circulated.

Infrastructures of value flow multiply not only horizontally, moving from one territory to another, but also cut through *spaces*; they bind geographically sparse communities, or allow different localities to exist in one place.

Bratton proposes the model of the stack to explain the layered stratification of digital technologies from worldwide computational *metainfrastructures* to single user devices; to depict the stack is to identify not only the machines and wires that form its grids, but also the "still-embryonic geopolitical institutions and social systems" (Bratton, 2016, p. 38) that produce and are reproduced by them. Nation-states as jurisdictional units are not done with, but their borders are transcended, reinforced or redefined by coexisting technologically exerted governance systems.

The coexistence of multiple digital value transfer infrastructures – some being an expression of national sovereignty, and contributing to its self-reinforcement (CBDCs); others becoming a locus of contestation and conflict among jurisdictions (SWIFT[173], INSTEX[174]); still others developing at

173 The use of SWIFT as a tool for the expression of (supra-)national sovereignty in international conflicts is showcased by the exclusion of Russia from the payment system in the aftermath of the invasion of Ukraine, based on a decision by the European Commission.

174 See: de Goede & Westermeier, 2022.

different layers of the stack, expressing the agency of other, non-state groups (platforms' payment systems, local alternative currencies, cryptocurrencies, NFTs, in-game currencies, etc.) – is a telling exemplification of how digital infrastructures enable new social institutions, creating new pathways for economic experiments and geopolitical organization.

The chapters of this thesis have inquired both the ways in which the state can predicate its jurisdictional power on and through technological infrastructures, and the ways in which technological infrastructures designed and governed by non-state actors exert powers that resemble what traditionally are considered state functions. Vis-à-vis worldwide, open-source networks of value flow like Bitcoin, credit systems enabled by global platforms, or small-scale experiments like the REC, state power does not lose its territory. Yet, power is partially deterritorialized, and the state is forced to rethink its functions in light of, and in response to, a plurality of agencies that negotiate spaces of economic and political life inside and outside of their territory.

That states and their institutions are reforming themselves along the layers of the digital stack is evident in the financial domain. Banking services are increasingly less territorially bound: mobile banking is offered to individuals irrespectively of their country of residency. The localization of consumers/users of financial services is not based on residence certificates but on geolocalization, as determined by device settings rather than state-issued documents. This is more than a bureaucratic detail: it signals that the bureaucratic criteria around which territorial states are organized is giving way to new forms of control institutionalized and enabled by different actors and technologies. As technologies of datafication explicate functions that are typical of state administration, fast data collection replaces traditionally slow bureaucratic processes, and the global reach of digital platforms solves issues of cross-border standardization.

As emerges from the exploratory empirical study in Chapter 5, the necessity of safeguarding variously defined ideas of *public good* against private interests in the construction of digital value transfer infrastructures is felt by social and political institutions at various levels of governance, from local civil society groups to European policymakers. Co-ops, state-run platforms, Urban

Digital Platforms (Chiappini, 2020), and self-sovereign technologies intended for and run by citizens are just some of the models proposed to posit non-extractive, no-profit, decentralized digital infrastructures at the center of public life.

A ceremonial and strategic manifestation of national institutions' efforts to maintain their legacy in the age of planetary scale computation is the development of Central Bank Digital Currencies. The introduction of CBDCs would not only safeguard states' monetary sovereignty against private money issuers; it would also have important, yet to be fully understood, geopolitical effects, as, for example, they might allow state currencies to be held by digital accounts regardless of their geographical location, opening an unprecedented currency competition at a global scale.

As local and global sociotechnical developments are co-constitutive of and in constant negotiation with each other, so are the value systems that they produce. The question of what will be the locus, and the scale at which the governance of future value transfer infrastructure will unfold, is a question with multiple, speculative possible answers. The geography of digital value transfer infrastructures will likely be multilayered, territorialized as it unfolds in specific physical locations, but entangled with larger, regional or global technological and institutional infrastructures that allow other powers to interfere. The supranational architecture of SWIFT, and the global platform, governed by the Bank of International Settlements, that could bundle CBDCs in the same governance structure, are both examples of how power can be dislocated and re-institutionalized at different scales through the constitution of information infrastructures.

The various scales at which value systems unfold do not necessarily result in a competition between new agencies and old sovereignties over the same space; rather, agencies can coexist, creating new localities and political spaces within the same territories. The question, for the legal system, is whether it is capable of tolerating, if not nurturing, such plurality of agencies without undermining its own fundamental functions.

The answer that Chapter 5 of this thesis suggests is a positive one. Municipal or local currencies created to respond to localized public interest do not

position themselves outside of the euro; they neither bypass nor threaten European monetary sovereignty. They simply actualize a political interest that the larger scale technocratic institutions like the ECB do not endorse. Circumscribing smaller communities, narrower economic circles, and digital infrastructures built as public utilities at different scales can allow the mobilization and predicament of public interests that global commercial platforms and state institutions fail to realize. As such, the possibility to articulate and mobilize a multiplicity of media and architectures for value transfer, even when they are not independent from larger-scale value transfer systems, allows the expression of the agencies of different groups and the flourishing of different economic cultures.

The conclusion of Chapter 5, therefore, is that agency in the construction of digital infrastructures that serve fundamental public functions – such as those enabling value transfer – should be allowed to move across different scales of political and economic institutions. Municipalities, if not even smaller political units, or non-geographically defined such units can, in fact, become venues of stable cooperation among a plurality of actors interested in the construction of technologies that respond to variously defined and negotiable ideas of public interest.

Imagining something else: imperfection, plurality, re-localized agency

Issues of online privacy are not solvable without changing the economic institutions that dominate digital commerce and communication. For such a change to take place, regulators should shift the imaginaries that guide their policymaking in the construction of digital infrastructures. They should, in particular, move away from imaginaries of technological environments imprinted on, and informed by, global commercial platforms. A shift in imaginaries cannot take place without the flourishing of diverse technological ecosystems and solutions, which offer alternative visions of possible technological futures. Such diversity and multiplicity is needed in order to reflect and express the agency, the political intention, and the ideas of common good that pertain to political and social institutions of various dimensions and geographical dispersion; communities that are circumscribed according to various criteria, beyond those of national liberal-democratic representation.

In more practical terms, this thesis advocates that the legal construction of privacy should overcome the notion that computerized interactions necessarily function by continuously forming trails of data referring to "identified/identifiable natural persons" (GDPR). This construction, in fact, reflects the configuration of information systems as they have evolved in parallel to neoclassical economic theories, conceptualizing and institutionalizing identity as the atomic separation of finite individuals (Agre, 1999). This conceptual move demands, first of all, a recognition that the digital affordances of the expression of identity and the subsequent notions of privacy in the digital realm reflect particular political economies and their subsequent identity politics.[175]

Decentralized cryptographical protocols, starting from Chaum's system for pseudonymous digital cash, represent an alternative architecture that protects privacy by allowing a going beyond of the need to "tell users apart" in computer interactions. These experiments, from Chaum's academic projects to the latest iteration of decentralized cryptocurrencies and self-sovereign identity solutions,[176] constitute a counter-imaginary in terms of system design. They not only allow an organization of systems of digital value transfer based on different architectures of trust and power (Becker & Bodó, 2021), but they also materialize different normative models for online interactions and digital self-representation.

In 1999, Agre warned us that, in order to fulfill their promises, these kinds of proposals would need to be "integrated within the larger institutional world, including business models, regulatory systems, contractual language and social customs" (Agre, 1999, p.4). The open-source blockchain ecosystem, as well as initiatives such as Commoncoin and even the digital euro, as discussed in Chapter 5, can be seen as attempts to develop the infrastructures for such integration to take place.

Organizing online environments in which contractual execution is guaranteed without the need to link users to their identities would deeply undermine

175 On the colonial and capitalistic origins of identity politics, see: Preciado P. (2020) Chronique «interzone». Inexistants. In Libération. For counter-narratives and resistance practices against the imposition of digital identity affordances based on coded categorizations, see: Russell L. (2020) Glitch Feminism: A Manifesto. Verso Books.

176 See Giannopoulou, 2023 – forthcoming.

digital platforms' business models. The question is which political institutions are truly willing to construct such a model. While Chapter 4 has underlined the lack of commitment of European policymakers to challenging the platform economy, Chapter 5 has exposed initiatives of digital infrastructures built as public utilities. The latter are developed as possible alternatives to commercial digital infrastructures that are increasingly perceived as architectures of control, designed for the optimized functioning of global, extractive capitalistic enterprises (Deleuze, 1992; Pistor, 2019).

The rise of multiple, contested, delocalized and vertically overlapping digital value transfer infrastructures – originating within or outside legal institutions – demonstrate the need to de- center and re-organize our conceptions of the political and economic spaces through which value can flow. Code expresses the prerogatives of different groups – social, economic and political actors (Nakamura, 2002). Law should step in to limit technological monopolies, shield individual rights against the interests of extractive commercial platforms, and even predicate itself through its own digital architectures. But a democratic legal system should also allow a plurality of agencies to express themselves. Such expression can include contributing to the construction of the digital infrastructures that govern public lives.

Encouraging the flourishing of diverse digital infrastructures (Hui, 2020), including value transfer infrastructures, involves taking up risk. The dynamic of mutual conflict and integration between the legal systems and digital infrastructures, governed by powers that lie outside of them, is a constant search for a point of balance. This perpetual search might result in temporary, occasional, geographically circumscribed events of alignment, and recurrent, prolonged situations of misalignment.

Yet, plurality is ultimately a necessary antidote to the totalizing effects of surveillance apparatuses enabled by datafication and algorithmic enforcement. It is the alternative to the flattening of society into a mass of compliant *dividuals* (Deleuze, 1992). It is the way to resist the centralization of power that is distinctive of the platform model, which is increasingly organizing all sectors of economy and culture, with evident detrimental effects on both.

In conclusion, against perfect enforcement, the possibility of an *outside* in the landscape of potential digital architectures needs to remain imaginable and designable. In the co-development of legal systems and digital infrastructures that are core to public life, conflicts are productive. Negotiations, ruptures, and exceptions are constitutive of the unending process of mutual reinforcement, and mutual containment, in which a plurality of agencies – expressed through legal institutions, symbolic systems, as well as information and media structures – are entangled.

ANNEXES

ANNEX 1: LIST OF ANALYZED DOCUMENTS (CHAPTER 4)

Institution	Year	Document title	Code name
EU Parliament	2014-2019	FinTech: the influence of technology on the future of the financial sector	EPFin2014-19
EU Parliament	2017	Resolution on Fintech	EPFin2014-19
EU Commission	2018	Press release: Payment services: Consumers to benefit from cheaper, safer and more innovative electronic payments	CommPress2018
EU Parliament	2021	Legislative Train (Action plan on fintech including a strategy on an integrated EU Payments market).	EPTrain2021
EU Commission	2017	Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions Consumer Financial Services Action Plan: Better Products, More Choice	CommCons2017
EU Commission	2018	Fintech Action Plan	CommFin2018
EU Commission	2018	Press release: FinTech: Commission takes action for a more competitive and innovative financial market	CommFin2018 (2)
EU Commission	2018	Press Release (Fintech Action Plan)	CommFin2018 (3)
EU Commission	2018	Factsheet (Fintech Action Plan)	CommFacts2018

EU Commission	2018	Annex to Fintech Action Plan	CommAnnex2018
EU Commission	2018	Payment services: Consumers to benefit from cheaper, safer and more innovative electronic payments	CommPay2018
EU Commission	2019	Your rights when making payments in Europe (leaflet)	CommRights2019
EU Commission	2019	Payments Services Directive (PSD2): The European Commission welcomes the adoption of a Joint Statement by three European Credit Sector Associations (ECSAs) and representatives of two Third Party Providers organizations on PSD2 implementation	CommPSD22019
EU Commission	2020	Communication on a Retail Payments Strategy for the EU	CommComm2020
EU Commission	2021	Consultation on a new Digital Finance strategy	CommCons2021
EU Commission	2021	Request to EBA, EIOPA and ESMA for technical advice on digital finance and related issues	CommReq2021
EU Commission, ECB	2021	Joint statement by the European Commission and the European Central Bank on their cooperation on a digital euro	CommECBjs2021
EBA	2017	Report on innovative uses of consumer data by financial institutions	EBARep2017
EBA	2018	The EBA's fintech roadmap: Conclusions from the consultation on the EBA's approach to financial technology (fintech)	EBAConcl2018

EBA	2019	Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2	EBAOp2019
EBA	2019	EBA responses to issues XXI to XXVI raised by participants of the EBA Working Group on APIs under PSD2	EBAResp2019
EBA	2019	EBA clarifications to issues I to III raised by participants of the EBA Working Group on APIs under PSD2	EBACla2019
EBA	2019	EBA responses to issues IV to VII raised by participants of the EBA Working Group on APIs under PSD2	EBAResp2019 (2)
EBA	2019	EBA responses to issues VIII to XIII raised by participants of the EBA Working Group on APIs under PSD2	EBAResp2019 (3)
EBA	2019	EBA responses to issues XIV to XX raised by participants of the EBA Working Group on APIs under PSD2	EBAResp2019 (4)
EBA	2019	EBA report on the impact of fintech on payment institutions and e-money institutions' business models	EBARep2019
EBA	2021	Opinion of the European Banking Authority on supervisory actions to ensure the removal of obstacles to account access under PSD2	EBAOp2021
ECB	2020	Press Release: ECB welcomes initiative to launch new European payment solution	ECBPress2020
ECB	2020	Interview Christine Lagarde: The future of money – innovating while retaining trust	ECBInt2020
ECB	2021	Interview Fabio Panetta: Evolution or revolution? The impact of a digital euro on the financial	ECBInt2021

ECB	2021	The Eurosystem's retail payments strategy	ECBStra2021
ECB	2021	Eurosystem report on the public consultation on a digital euro	ECBStra2021
ECB	2021	Eurosystem report on the public consultation on a digital euro	ECBRep2021
ERPB	2014-2015	Annual report	ERPB2014-15
ERPB	2015-2016	Annual report	ERPB2015-16
ERPB	2016-2017	Annual report	ERPB2016-17
ERPB	2017-2018	Annual report	ERPB2017-18
ERPB	2018-2019	Annual report	ERPB2018-19
ERPB	2020	ERPB reaction to the Commission's consultation on a retail payments strategy for the EU	ERPBreact2020
EFIP	2017	Statement following the first meeting of the European Forum for Innovation in Payments held on November 29, 2017	EFIP2017
EFIP	2019	Statement of the second meeting of the European Forum for Innovation in Payments held on November 25, 2019	EFIP2019

ANNEX 2: CODEBOOK - CODE GROUPS AND THE RELATIVE SUB-CODES ASSOCIATED WITH EACH OF THE GROUPS (CHAPTER 4)

Feelings/attitude	acceleration, acceptance, awareness, boosting innovation, complexity, confidence, convenience, fitness/preparedness/readiness for digital age, good will, impetus/momentum, need for action, reassurance (need of), reluctance, uncertainty, urgency, welcoming new developments.
Change/transformation	becoming the new normal, Brexit, catalyst for change, change of market structure, change of payment instruments, changing business models, changing consumer habits/preferences, changing our lives, COVID-19, digital euro as natural evolution, digitalization, digitalization of economy, digitalization of payments, digitalization of public services, future (-oriented/-proofness), impact of technology in finance, innovation, modernization, momentum, natural evolution of PSD2, new technologies, new types of actors, shift in payment preferences, socioeconomic changes.
Risk/obstacles	biases and errors, concentration of power, counterfeiting and technical mistakes, dependency on technologies governed elsewhere, disabilities and old age, financial disruption, geographical limitedness, illicit activities, instability, internet coverage, obstacles/barriers, protection of central bank money, risks, speculation, stablecoins, targeted pricing, tax evasion, threat to sovereignty, vulnerability to international developments.
Benefits	fintech investments, businesses interests, consumers/citizens/societal interests and needs, cross-border payments, efficiency, EU financial autonomy, improve contractual terms for customers, inclusion, increase consumer choice, lower costs, meeting the mutual interest of stakeholders, opportunities of fintech innovation, stability, strengthening the banking industry, sustainability, targeted pricing, trust.
Market	acquisition of fintech firms by institutions, capital market union, change of market structure, changing business models, competing with cash and cards, competition, concentration of power, customer ownership, digital single market, e-commerce, economic impact of CBDC, global competition, global reach and impact of digital euro, impact of technology in finance, international role of the euro, investment, network effects, open asset sharing economy, open banking, open finance, private money, PSP's independence from banks.

Regulation/enforcement/supervision	adaptation of regulation to innovation, AML/CTF, authorization and licenses, balancing of interests, best practices, boosting innovation, breaking of supervisory silos, certificates, clarity of technical requirements, competition law, compliance, compound risk/holistic approach to regulation, consent, consistency of implementation, consolidated supervision, consumer and investor protection, consumer rights, cross-border cooperation, cybersecurity, data localization rules, difference of rules for banks and tech companies, DMA, e-IDAS, European Financial Transparency Gateway, formalization of payment security requirements, GDPR, governance arrangements, green deal data/environmental data, incentives, industry-led solutions, ISO, market-led standardization, money as a public good, no regulatory intervention, proprietary standards, PSD2, regulatory sandboxes, Regulatory Technical Standards, regulatory uncertainty, regulatory updates (need of), risk-based approach, same business same rule, sectorial regulation, service providers responsibility, spending limits, supervision/monitoring, technology neutral regulation, testing, uniformity of rules across EU, voluntary commitment.
Knowledge	awareness of disadvantages, consumer awareness, education, engagement with companies, familiarity, financial and digital literacy, information gathering, knowledge/understanding of technology, list of service providers, public consultation, research/preparatory work, supervision/monitoring, take-up of technical solutions.
Technological design	access to payers' account, access to payment systems, accessibility of payment infrastructure, anonymity, attractiveness, availability (to users), cash-like features, confidentiality, consumer-centric, efficiency, frictionless, integration, interoperability, large-scale processing, offline usability, openness, personalization, programmability, PSP's independence from banks, safe/secure, seamless (user experience), simplicity, speed, transparency, trust, usability, user-friendliness.
Actors	API evaluation group, ASPSPs, banking sector, BigTech, EU fintech laboratory, EU forum for innovation in payment, EU observatory and forum on blockchain, expert groups, financial institutions, intermediaries, mobile service providers, national authorities, new types of actors, NGOs, out of EU jurisdiction service providers, Payment Information Management Systems (PIMS), Payment Initiation Services (PIS), platforms, social media, start-ups, tech companies, third-party payment service providers.

Services	account information services (AIS), additional features and services, authentication, cloud services, cross-currency payments, crowdfunding, electronic signatures, instant payments, insurance, marketing, out of EU jurisdiction service providers, outsourcing of services, P2P mobile payments, payment initiation services (PIS), remittances, value-added services.
Infrastructure	access to payment accounts, accessibility of payment infrastructure, additional features and services, API, authentication, banks stepping in the back, cash (availability of), CBDC/digital euro, cloud computing infrastructure, communication infrastructure, complementarity (of payment methods), cross-border payments, decentralized infrastructure, dematerialization (of money), digital identity, distribution networks, easy provider switching, fragmentation (avoidance of), geographical limitedness/local solutions, information exchange, information repository, integrated data pools, integration, intermediation, interoperability, large-scale processing, multi-party infrastructure, open banking, outsourcing of services, pan-European reach/interoperability, pan-European data access, platforms, point-of-sale /point-of-interaction, request-to-pay functionality, SCT Inst scheme, SEPA, SEPA API access scheme, SEPA Proxy Lookup, standardization, technical migration, technological barriers (absence of).
Technologies	AI, algorithms, automation, behavior prediction, big data analytics, blockchain/DLTs, Bluetooth, cloud computing infrastructure, crypto-assets, cryptography, generic QR code, hardware solutions/devices, interfaces, IoT, mobile technologies, plastic cards, proximity technologies, RegTech, remote identification techniques, risk-based authentication, robo-advice, stablecoins, strong customer authentication.
Data	abuse of personal information for commercial purposes, access to consumer data, automated data processing, biases and errors, big data analytics, biometric data, common financial data space, consent, data-driven innovation/business models, free flow of personal data, GDPR, green deal data/environmental data, integrated data pools, money as (digital) memory, pan-European data access, personal data, privacy/data protection, selective privacy.

ANNEX 3: LIST OF INTERVIEWS (CHAPTER 5)

ID	Country	Organization and Use Cases	Role (may be redacted to ensure anonymity)
Interviewee 1	Netherlands	ECB – Digital euro	Researcher/advisor
Interviewee 2	Netherlands	DNB – Digital euro	Senior economist
Interviewee 3	Netherlands	ECB – Digital euro	Technology and Innovation expert
Interviewee 4	Germany	ECB – Digital Euro	Legal Services
Interviewee 5	Spain	Novact - REC	Consultant, team member
Interviewee 6	Spain	Novact - REC	Economist
Interviewee 9	Spain	Novact - REC	Project coordinator
Interviewee 11	Spain	Novact - REC	Project coordinator
Interviewee 12	Spain	Barcelona City Council - REC	Policymaker
Interviewee 13	-	Dyne.org – CommonCoin	Co-founder
Interviewee 14	UK	Dyne.org – CommonCoin	Software developer/ researcher

BIBLIOGRAPHY

ÁVILA PINTO R. (2018) Digital sovereignty or digital colonialism? in New tensions of privacy, security and national policies, Sur 27. https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/

ADHAMI S., GIUDICI G., MARTINAZZI S. (2018) Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings. Journal of Economics and Business,100.

AGHA A. (2017). Money Talk and Conduct from Cowries to Bitcoin. Signs and Society, 5(2), 293–355. https://doi.org/10.1086/693775.

AGRE P.E. (1999) The Architecture of Identity: Embedding Privacy in Market Institutions. Information, Communication and Society 2(1), 1999, pp. 1-25.

AMATO M. (2016) L'enigma della moneta. Orthotes, Milano.

AMOORE L., DE GOEDE M. (2021). Datawars: reflections twenty years after 9/11, Critical Studies on Terrorism, 14:4, 425-429, DOI: 10.1080/17539153.2021.1982117.

AMSDEN R., SCHWEIZER D. (2018) Are Blockchain Crowdsales the New "Gold Rush"? Success Determinants of Initial Coin Offerings, 2nd Emerging Trends in Entrepreneurial Finance Conference. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3163849.

BARBROOK R, CAMERON A. (1995) The Californian ideology. Sci Cult 1996; 6:44–72. DOI:10.1080/09505439609526455.

BECKER M., BODÓ, B. (2021). Trust in blockchain-based systems. Internet Policy Review, 10(2). https://doi.org/10.14763/2021.2.1555.

BELLANOVA R., DE GOEDE M. (2022) The algorithmic regulation of security: An infrastructural perspective. Regulation & Governance, 16: 102-118. https://doi.org/10.1111/rego.12338.

BENJAMIN W. (1968/2007). The Work of Art in the Age of Mechanical Reproduction. in Illuminations, ed. Hannah Arendt. New York: Schocken Books.

BERBER L.K., ATABEY A. (2021) Open banking & banking-as-a-service (BaaS): a delicate turnout for the banking sector. Glob Privacy Law Rev 2021; 2:59–82 Issue 1, pp. 59-82. https://doi.org/10.54648/gplr2021009.

BERNARD N., CAMPBELL-VERDUYN M. (2019) Understanding technological change in global finance through infrastructures. Rev Int. Polit. Econ, 26(5), 773–89. DOI:10.1080/09692290.2019.1625420.

BERNARDS N., CAMPBELL-VERDUYN M. (2019) Understanding technological change in global finance through infrastructures. Review of International Political Economy, 26:5, 773-789, DOI: 10.1080/09692290.2019.1625420.

BLASI CASAGRAN C. (2016) *Global data protection in the field of law enforcement: An EU perspective.* Routledge.

BODÓ B. (2021). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. New Media & Society, 23(9), 2668-2690.
BODÓ B., GIANNOPOULOU A. (2019) The Logics of Technology Decentralization - The Case of Distributed Ledger Technologies, in Ragnedda M. and Destefanis G. (eds.), Blockchain and Web 3.0: Social, Economic, and Technological Challenges. Routledge.
BORGESIUS F. Z., POORT J. (2021) Personalised Pricing: The Demise of the Fixed Price? *Data-Driven Personalisation in Markets, Politics and Law.* http://works.bepress.com/frederik-zuiderveenborgesius/64/.
BRATTON B.H. (2016) The Stack. On Software and Sovereignty. MIT Press.
BRAUN B, GABOR D. (2020) Central Banking, Shadow Banking, and Infrastructural Power. In: Mader P., Mertens D., van der Zwan N. (eds.). The Routledge International Handbook of Financialization, Abingdon: Routledge, 241-252.
BROMLEY S. (1999) The space of flows and timeless time: Manuel Castells's The Information Age', Radical Philosophy 097.
BUTERIN V. (2017) The Meaning of Decentralization. Medium. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.
CASTELLS M. (1996) The Rise of the Network Society: The Information Age: Economy, Society, and Culture. Wiley-Blackwell.
CATALINI C., GANS J.S. (2018) 'Initial Coin Offerings and the Value of Crypto Tokens', NBER Working Paper No. w24418 (2018), https://www.nber.org/papers/w24418.
CAVOUKIAN A. (2009). Privacy by Design: The 7 Foundational Principles.
CHAUM, D. (1983). Blind Signatures for Untraceable Payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds) Advances in Cryptology. Springer, Boston, MA. https://doi.org/10.1007/978-1-4757-0602-4_18.
CHAUM D. (1985) Security without Identification: Transaction Systems to Make Big Brother Obsolete. Communications of the ACM, 28, 1030-1044. https://doi.org/10.1145/4372.4373.
CHIAPPINI, L. (2020). The Urban Digital Platform: Instances from Milan and Amsterdam. Urban Planning, 5(4), 277-288. https://doi.org/10.17645/up.v5i4.3417.
COHEN J.E. (2019) Between truth and power: the legal constructions of informational capitalism. Oxford University Press.
CRISTOFARI B (2022). Bratton and the double movement of state platformization and platform institutionalization. La Deluziana, Issue 12.
CSERES K. (2005). Competition law and consumer protection. Kluwer Law Int BV; 49.
CSERES K. (2008) What has competition done for consumers in liberalised markets? Comp Law Rev 2008; 4(2):77–121. Available at SSRN: https://ssrn.com/abstract=1273611.
DELEUZE G. (1992) Postscript on the Societies of Control. The MIT Press. Vol. 59. pp. 3-7.

DELEUZE G., GUATTARI F. (1973) L'Anti-Œdipe. In *Introduction à la schizo-analyse.* de Minuit.
DELOITTE, (2018) After the dust settles - How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-the-impact-of-gdpr-on-the-financial-services.pdf.
DE FILIPPI P., WRIGHT A. (2018) Blockchain and the Law: The Rule of Code. Harvard University Press.
DE GOEDE M. (2021) Finance/security infrastructures. Review of International Political Economy, 28:2, 351-368, DOI: 10.1080/09692290.2020.1830832.
DE GOEDE M., WESTERMEIER C. (2022) Infrastructural Geopolitics. International Studies Quarterly, Volume 66, Issue 3, September 2022, sqac033, https://doi.org/10.1093/isq/sqac033.
DE NEDERLANDSCHE BANK (2020). Central Bank Digital Currency: Objectives, preconditions and design choice. https://www.dnb.nl/media/c3qgn4lk/202004_nr-_1_-2020-_-_central_bank_digital_currency_-_objectives-_preconditions_and_design_choices.pdf.
DIETER, M., TKACZ, N. (2020) The patterning of finance/security: a designerly walkthrough of challenger banking apps, computational culture 7. Available at: http://computationalculture.net/the-patterning-of-finance- security.
DODD N. (2016) The Social Life of Money. Princeton, NJ: Princeton University Press.
DOMMERING E. (2006). Regulating technology: code is not law. In Dommering E., Asscher L., (eds.) Coding Regulation. Essays on the Normative Role of Information Technology. Information Technology & Law Series.
DONNELLY M. (2016) Payments in the digital market: evaluating the contribution of payment services directive II. Comput Law Secur Rev. DOI:10.1016/j.clsr.2016.07.003.
DORIA L., FANTACCI L. (2018) Evaluating complementary currencies: from the assessment of multiple social qualities to the discovery of a unique monetary sociality. Quality and Quantity. 52. 1-24. 10.1007/s11135-017-0520-9.
DU PONT Q. (2019) Cryptocurrencies and Blockchains. Wiley.
EASTERLING K. (2014) Extrastatecraft: the power of infrastructure space. Verso.
EUBANKS V. (2017) Automating inequality: how high-tech tools profile, police, and punish the poor. New York: St. Martin's Press.
FARIA I. (2019) Trust, Reputation and Ambiguous Freedoms: Financial Institutions and Subversive Libertarians Navigating Blockchain, Markets, and Regulation, Journal of Cultural Economy, 12.
FATHAIGH R.Ó., VAN HOBOKEN J., VAN EIJK N. (2019) Mobile Privacy and Business-to-Platform Dependencies: An Analysis of SEC Disclosures. Journal of Business & Technology Law, 49.
FERRARI V. (2020) Tecnologie e geografie di potere delle piattaforme digitali: Libra. Kabul Magazine. https://www.kabulmagazine.com/tecnologie-geografiei-potere-piattaforme-digitali-libra/.

FERRARI V. (2020) Crosshatching Privacy: Financial Intermediaries' Data Practices Between Law Enforcement and Data Economy. European Data Protection Law Review, 6(4), 522-535.

FERRARI V. (2021). Introducing the glossary of decentralised technosocial systems. Internet Policy Review, 10(2). https://doi.org/10.14763/2021.2.1546.

FERRARI V. (2022) The platformisation of digital payments: The fabrication of consumer interest in the EU FinTech agenda, Computer Law & Security Review, Volume 45, 105687, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2022.105687.

FERRARI V., CHIAPPINI L. (2023) Digital geographies of power: The scale of digital money infrastructures, forthcoming: First Monday, Governance by Infrastructure Special Issue.

FERRARINI G., MACCHIAVELLO E. (2018) FinTech and Alternative Finance in the CMU: The Regulation of Marketplace Investing, in Busch D., Avgouleas E. and Ferrarini G. (eds.). Capital Markets Union in Europe. Oxford University Press.

FISCH C. (2019) Initial Coin Offerings (ICOs) to Finance New Ventures. Journal of Business Venturing, 34, 1-22. https://doi.org/10.1016/j.jbusvent.2018.09.007.

FUCHS C. (2021) The Digital Commons and the Digital Public Sphere: How to Advance Digital Democracy Today. Westminster Papers in Communication and Culture 16(1), pp. 9-26. DOI: https,://doi.org/10.16997/wpcc.917.

FUMAGALLI A. (2016) Grateful Dead Economy – La psichedelia finanziaria. AgenziaX.

GALLOWAY, A. R. (2006). Gaming: Essays on Algorithmic Culture (NED-New edition, Vol. 18). University of Minnesota Press. http://www.jstor.org/stable/10.5749/j.ctttss5p.

GEOFFREY I. (2004) The Nature of Money. Cambridge: Polity Press.

GIANNOPOULOU A., WANG, F. A. (2021) Self-sovereign identity. Internet Policy Review, 10(2). https://doi.org/10.14763/2021.2.1550.

GIANNOPOULOU A. (2023- forthcoming), Digital identity infrastructures: a critical approach of self-sovereign identity, in Digital Society, issue 4.

GIANNOPOULOU A., & FERRARI V. (2019). Distributed Data Protection And Liability On Blockchains. Internet Science: INSCI 2018 International Workshops. pp. 203-211. Lecture Notes in Computer Science; Vol. 11551. Springer.

GIDDENS A. (1990) *The consequences of modernity*. Stanford University Press.

GIDDENS A. (1984) *The Constitution of Society: Outline of the Theory of Structuration*, Cambridge: Polity Press.

GOANTA C., HOPMAN M. (2020). Crypto communities as legal orders. Internet Policy Review, 9(2). DOI: 10.14763/2020.2.1486.

GRAEBER D. (2011) Debt: The First 5,000 Years. Brooklyn, NY: Melville House.

GUYAN, K. (2022). Queer Data, Using Gender, Sex and Sexuality Data for Action. Bloomsbury Studies in Digital Cultures.

HACKER P., THOMALE C. (2018) Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law, 15 European Company and Financial Law Review. pp. 645-696.

HAN B. (2015). The transparency society, Stanford University Press.

HAJER M. (1995) The politics of environmental discourse: ecological modernization and the policy process. Oxford: Oxford University Press.

HART K. (1986) Heads or tails? Two sides of the coin. Man (New Series) 21(4).

HAUPT J. (2021) Facebook futures: Mark Zuckerberg's discursive construction of a better world. New Media Soc; 23(2):237–57. DOI:10.1177/1461444820929315.

HELBERGER N. (2006) Code and (Intellectual) Property. In Dommering E., Asscher L., (eds.) Coding Regulation. Essays on the Normative Role of Information Technology. Information Technology & Law Series.

HELBERGER N., LOOS M.B.M., GUIBAULT L., ET AL. (2013) Digital content contracts for consumers. J Consum Policy; 36:37–57. DOI:10.1007/s10603-012-9201-1.

HELLEINER E. (2003) The Making of National Money: Territorial Currencies in Historical Perspective. Ithaca: Cornell UP.

HERIAN R. (2019). *Regulating Blockchain: Critical Perspectives in Law and Technology*, Routledge.

HILDEBRANDT M. (2009) Profiling and AML. In Rannenberg K., Royer D., Deuker A. *The Future of Identity in the Information Society. Challenges and Opportunities.* Springer.

Hong S. (2020) Technologies of Speculation: The limits of knowledge in a data-driven society. NYU Press.

HUI Y. (2020) Cosmotechnics, Angelaki, 25:4, 1-2, DOI: 10.1080/0969725X.2020.1790828. ICO Watch List, 'ICO Statistics - By Year (2018)', ICO Watchlist (2019), https://icowatchlist.com/statistics/year.

INGHAM G. (2004) The Nature of Money. Cambridge, UK: Polity.

Ippolita (2017) Le tecnologie del Dominio. Lessico minimo di autodifesa digitale, Maltemi Editore, Milano.

Irrera A., Withers I., (2021) Banks beware, Amazon and Walmart are cracking the code for finance, Reuters; https://www.reuters.com/business/finance/ banks-beware-outsiders-are-cracking-code-finance-2021-09-17.

ISLAMI S.Y. (2011) The Opacity of Glass. Rethinking Transparency in Contemporary Architecture. International Journal Of Architecture and Urban Development Vol.1, No.2, Autumn 2011.

JANSSEN H., COBBE J., SINGH J. (2020) Personal information management systems: a user-centric privacy Utopia? Internet Policy Rev; 9(4):1–25. DOI:10.14763/2020.4.1536.

JASANOFF S., KIM S.H. (2009) Containing the atom: sociotechnical imaginaries and nuclear power in the United States and South Korea. Minerva;47:119. DOI:10.1007/s11024-009-9124-4.

JONES H. (2019) Facebook's Libra falls into 'big gap' in EU rules: regulator. Reuters-Technology News. https://www.reuters.com/article/us-eu-banks-moneylaundering/facebooks-libra-falls-into-big-gap-in-eu-rules-regulator-idUSKCN1VQ1OY.

JONES P. (2021) Work without the worker - labour in the age of platform capitalism. Verso; ISBN 9781839760433.

KHARIF O. (2018). Bitcoin's Use in Commerce Keeps Falling Even as Volatility Eases. Bloomberg. https://www.bloomberg.com/news/articles/2018-08-01/bitcoin-s-use-in-commerce-keeps-falling-even-as-volatility-eases.

KING M.R., NESBITT R.W. (2020) The technological revolution in financial services: how banks. Fintechs, and Customers Win Together, University of Toronto Press.

LAGARDE C. (2020) The Future of Money – innovating while retaining trust, L'ENA hors les murs.

LANGLEY P., LEYSHON A. (2020) The Platform Political Economy of FinTech: Reintermediation, Consolidation and Capitalisation. New Political Economy, DOI: 10.1080/13563467.2020.1766432.

LANGLEY P., LEYSHON A. (2021) The platform political economy of FinTech: reintermediation, consolidation and capitalisation. New Polit Econ; 26(3):376–88. DOI:10.1080/13563467.2020.1766432.

LARKIN B. (2013) The politics and poetics of infrastructure. Annu Rev Anthropol; 42:327–43 https://www.annualreviews.org/doi/ abs/10.1146/annurev- anthro- 092412- 155522.

LASSWELL H. (1936) Politics: Who Gets What, When, How (Cleveland/New York).

LAUER J. (2017) Creditworthy. A History of Consumer Surveillance and Financial Identity in America. Columbia University Press.

LEFEBVRE H. (1974) La production de l'espace. Paris. Anthropos, 420.

LEHDONVIRTA V., VIDAN G. (2019) Mine the Gap: Bitcoin and the Maintenance of Trustlessness, 21 New Media and Society. pp. 42–59.

LEISER M., CUSTERS B. (2019) The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680. European Data Protection Law Review 5(3).

LIAO T., ILIADIS A. (2021) A future so close: mapping 10 years of promises and futures across the augmented reality development cycle. New Media Soc; 23(2):258–83. DOI:10.1177/1461444820924623.

LITAN R.E., POMERLEANO M., SUNDARARAJAN V. (2002) Financial sector governance: the roles of the public and private sectors. Brookings Institution Press.

LUHMANN N. (2004) Law as a Social System. Oxford University Press.

LUX M., SHACKELFORD M. (2020) The new frontier of consumer protection: financial data privacy and security, M-RCBG associate Working Papers Series No. 135, last accessed June 10, 2020.

LYNGGAARD K. (2019) Discourse analysis and European Union politics. Palgrave Studies in European Union Politics.

MAGER A., KATZENBACH C. (2020) Future imaginaries in the making and governing of digital technology: multiple, contested, commodified. New Media Soc. DOI:10.1177/14614448209 29321.

MAK, V. (2015) The consumer in European Regulatory private law. Leczykiewicz D., Weatherill S. (eds), The Image of the Consumer in EU Law: Legislation, Free Movement and Competition Law (Hart Publishing) 381-400, Tilburg Private Law Working Paper Series No. 05/2015, Available at SSRN: https://ssrn.com/abstract=2600474.

MARKHAM A. (2020) The limits of the imaginary: challenges to intervening in future speculations of memory, data, and algorithms. New Media Soc. DOI:10.1177/1461444820929322.

MARTIN A. (2019) Mobile Money Platform Surveillance. Surveillance and Society. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12924.

MARX K. (1844) Comments on James Mill. Éléments D'économie Politique.

MATTILA J., SEPPÄLÄ T., LÄHTEENMÄKI I. (2018) Who holds the reins? – Banks in the crossfire of global platforms; ETLA Report No 86. https://pub.etla.fi/ETLARaportit-Reports-86.pdf.

MAY T. (1992) The Crypto Anarchist Manifesto. https://www.activism.net/cypherpunk/crypto-anarchy.html.

MEJIAS U. A., (2019) Couldry N. Datafication. Internet Policy Rev; 8(4). DOI:10.14763/2019.4.1428.

MICKLITZ H. W., Weatherill S. (1993) Consumer policy in the European Community: before and after Maastricht. J Consum Policy; 16:285–321 Kluwer Academic Publishers.

MONRAT, A. A., SCHELÉN, O. AND ANDERSSON, K. (2019) A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities. IEEE Access, 7, 117134-117151.

Muellerleile C. (2021) The Place of Money in History. The SAGE Handbook of Historical Geography, Volume: 1, Part III, Chapter 12

MUKERJI C. (2010) The territorial state as a figured world of power: strategics, logistics, and impersonal rule. Social Theory; 28(4): 402–24.

MULDOON J. (2022) Platform Socialism: How to Reclaim our Digital Future from Big Tech. Pluto Press.

MUSIANI F., DE NARDIS L. (2016) Governance by Infrastructure. In The turn to infrastructure internet governance, edited by Musiani F., Cogburn D. L., De Nardis L., Levinson N.

MÜTZEL S. (2021) Unlocking the payment experience: future imaginaries in the case of digital payments. New Media Soc; 23(2):284–301.

NAKAMOTO S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf.

NAKAMURA L. (2002) Cybertypes: Race, Ethnicity, and Identity on the Internet. Routledge. ISBN 9780415938372.

NISHIBE M. (2016) The Enigma of Money. Springer.

NOBLE S.U. (2018) Algorithms of Oppression. How Search Engines Reinforce Racism. NYU Press.
O'NEIL C. (2016) Weapons of Math Destruction How Big Data Increases Inequality and Threatens Democracy. Crown Books.
PASQUALE F. (2015) The Black Box Society. The Secret Algorithms That Control Money and Information. Harvard.
PERE M., ELKIN-KOREN N. (2015) Black box tinkering: beyond disclosure in algorithmic enforcement. Florida Law Review 69(181).
PISTOR K. (2019) The Code of Capital: How the Law Creates Wealth and Inequality. Princeton University Press.
PISTOR K. (2020) Statehood in the digital age. Constellations. 27: 3–18. https://doi.org/10.1111/1467-8675.12475.
PLANTIN J.C., LAGOZE C., EDWARDS P.N., SANDVIG C. (2018) Infrastructure studies meet platform studies in the age of Google and Facebook. New Media Soc; 20(1): 293–310 2018. DOI:10.1177/1461444816661553.
POHLE J., THIEL T. (2020) Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532.
POELL T., NIEBORG D., VAN DIJCK J. (2019) Platformisation. Internet Policy Rev;8(4). DOI:10.14763/2019.4.1425.
POLANY K. (1944) The Great Transformation. The Political and Economic Origins of Our Time. Beacon Press.
PORTER T.M. (1996) Trust in Numbers: The Pursuit of Objectivity in Science and Public Life. Princeton University Press.
PRASAD E. S. (2021) The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance. The Belknap Press of Harvard University Press.
PRECIADO P. (2020) Chronique «interzone». Inexistants. In Libération. For counter-narratives and resistance practices against the imposition of identity through coded categorization.
PROTOCOL LABS, 'Filecoin: A Decentralized Storage Network', Filecoin (2017), https://filecoin.io/filecoin.pdf.
REDEALLI E. (2016) La moneta come segno, in Nuovi usi di vecchi concetti, edited by Striano M., Oliverio S., Santarelli M., Mimesis/Eterotopie.
REIJERS W., COECKELBERGH M. (2016) The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies. Philosophy & Technology, 1–28. https://doi.org/10.1007/s13347-016-0239-x.
REISCH L.A., MICKLITZ H.W. (2006) Consumers and deregulation of the electricity market in Germany. J Consum Policy; 29:399–415. DOI:10.1007/s10603-006-9016-z.
RAMIRO, A., DE QUEIROZ, R. (2022) Cypherpunk. Internet Policy Review, 11(2). https://doi.org/10.14763/2022.2.1664.

ROHR J., WRIGHT A. (2017) Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets, Cardozo Legal Studies Research Paper.

ROSENBACH E., MANSTED K. (2019) The Geopolitics of Information. Belfer Center For Science And International Affairs.

RUSSELL L. (2020) *Glitch Feminism: A Manifesto.* Verso Books

SADOWSKI J. (2019) When data is capital: datafication, accumulation, and extraction. Big Data Soc. DOI:10.1177/2053951718820549.

SAX M. (2021) Between empowerment and manipulation: the ethics and regulation of for-profit health apps; Kluwer, Amsterdam.

SCOTT C.J. (1998) Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed. Yale University Press.

SCHEBESTA, H. (2018). Content Analysis Software in Legal Research: A Proof of Concept Using ATLAS.ti. Tilburg Law Review, 23(1), 23-33. https://doi.org/10.5334/tilr.1.

SRNICEK N. (2017) Platform capitalism. Polity.

STAR S.L. (1999) The Ethnography of Infrastructure." American Behavioral Scientist 43, no. 3 (1999): 377–91. https://doi. org/10.1177/00027649921955326.

STEINBERG M. (2019) The platform economy. How Japan transformed the consumer internet. Minneapolis: University of Minnesota Press.

SWARTZ L. (2020) New Money: How Payment Became Social Media. Yale University Press.

THALER R.H., SUNSTEIN R. (2008) Nudge: improving decisions about health, wealth, and happiness. Yale University Press.

VAN DE DONK W., LOADER B.D., NIXON P.G., RUCHT D. (2004) Cyberprotest: New Media, Citizens and Social Movements. 1-276. 10.4324/9780203644225.

VAN DER LINDEN J.M., BOLLEN T. (2022) De strijd om het digitale geld is losgebarsten. Follow the Money at: https://www.ftm.nl/artikelen/de-strijd-om-het-digitale-geld-is-losgebarsten.

VAN DIJCK J., NIEBORG D., POELL T. (2019) Reframing platform power. Internet Policy Rev;8(2). DOI:10.14763/2019.2.1414.

VAN DOORN N. (2014) The Neoliberal Subject of Value: Measuring Human Capital in Information Economies. Cultural Politics; 10 (3): 354–375.

VAN PAASSEN (2020). Het is bijna gedaan met de briefjes en munten (maar nog niet helemaal). De Volkskrant, February 2020. https://www.volkskrant.nl/nieuws-achtergrond/het-is-bijna-gedaan-met-de-briefjes-en-munten-maar-nog-niet-helemaal~bc49ebab/?referer=https%3A%2F%2Fwww.google.com%2F.

VIDAN G. (2020) Checks and balances: publics, interests, and the development of electronic fund transfers in 1970s US. IEEE annals of the history of computing. Computing Capitalisms; vol. 42, no. 3, pp. 11-25, 1 July-Sept. DOI:10.1109/MAHC.2020.3008921.

VOGEL T. (2010). EU, US sign SWIFT agreement - MEPs' demands for changes accepted. Politico. https://www.politico.eu/article/eu-us-sign-swift-agreement/.
WALCH A. (2019) Deconstructing "Decentralization": Exploring the Core Claim of Crypto Systems, in Brummer C. (ed.), Crypto Assets: Legal, Regulatory and Monetary Perspectives. Oxford Academic. https://doi.org/10.1093/oso/9780190077310.003.0003.
WEINER A. (2022) Money in the Metaverse. The New Yorker: https://www.newyorker.com/news/letter-from-silicon-valley/money-in-the-metaverse.
WERBACH K. (2018) The Blockchain and the New Architecture of Trust. The MIT Press.
WESTERMEIER C. (2020) Money is data – the platformization of financial transactions, Information, Communication & Society, 23:14, 2047-2063, DOI: 10.1080/1369118X.2020.1770833.
Wilhelmson T. (1998) Consumer law and the environment: from consumer to citizen. J Consum Policy; 21:45–70.
WORLD ECONOMIC FORUM (2018). The Appropriate Use of Customer Data in Financial Services. http://www3.weforum.org/docs/WP_Roadmap_Appropriate_Use_Customer_Data.pdf.
YERMACK D. (2015) Is Bitcoin a Real Currency? An Economic Appraisal, in D.L. Kuo Chuen (ed.), Handbook of Digital Currency. Elsevier.
YEUNG K. (2017). Algorithmic Regulation: A Critical Interrogation. Regulation and Governance 12(4).
YEUNG K. (2018). Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law. Modern Law Review 82(2) 207-239.
ZETZSCHE D.A., ARNER D.W., BUCKLEY R.P., WEBER R.H. (2019). The future of data-driven finance and RegTech: lessons from EU Big Bang II. European Banking Institute Working Paper Series 2019/35.
ZHAI G. (2018) How Much Does It Really Cost to Do an Initial Coin Offering?. Medium. https://medium.com/blockchain-review/ico-budgets-how-much-does-it-really-cost-to-do-an-initial-coin-offering-eb1031e8d893.
ZICCARDI G. (2013). Resistance, Liberation Technology and Human Rights in the Digital Age. In Law, Governance and Technology Series, Springer.
ZUBOFF S. (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Publicaffairs.

LEGISLATION

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Payment Service Directive 2).

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (5th Anti-Money Laundering Directive).

Directive (EU)2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of Union consumer protection rules.

Directive (EU) 2003/71/EC of the European Parliament and of the Council of 4 November 2003 on the prospectus to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC, [2003] OJ L 345/64.

Directive (EU) 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, [2009] OJ L 267/7 (Electronic Money Directive).

Directive 2013/50/EU of the European Parliament and of the Council of 22 October 2013 amending Directive 2004/109/EC of the European Parliament and of the Council on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market, Directive 2003/71/EC of the European Parliament and of the Council on the prospectus to be published when securities are offered to the public or admitted to trading and Commission Directive 2007/14/EC laying down detailed rules for the implementation of certain provisions of Directive 2004/109/EC, [2013] OJ L 294/13.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law enforcement Directive).

Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, [2014] OJ L 173/349 (Directive 2014/65/EU).

European Parliament resolution of 17 May 2017 on FinTech: the influence of technology on the future of the financial sector (2016/2243(INI)) https://www.europarl.europa.eu/doceo/document/TA-8- 2017-0211_EN.html.

European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)).

Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 2022/1925 of the European Parliament and of The Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

Regulation 2017/1129/EU of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC, [2017] OJ L 168/12 (Regulation No. 2017/1129/EU).

Regulation 596/2014/EU of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, [2014] OJ L 173/1.

Regulation 600/2014/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No. 648/2012, [2014] OJ L 173/84 (Regulation N. 600/2014/EU).

Regulation No. 909/2014/EU of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012, [2014] OJ L 257/1.

Securities And Exchange Commission (SEC), 'Release No. 81207/2017: Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO', *SEC* (2017), https://www.sec.gov/litigation/investreport/34-81207.pdf.

United States Securities Exchange Act (1934).

SOFT LAW, REPORTS, POLICY DOCUMENTS

Assemblée nationale (2019) Rapport d'information en conclusion des travaux d'une mission d'information relative aux monnaies virtuelles. www.assemblee-nationale.fr/dyn/15/rapports/cion_fin/l15b1624_rapport-information.

Bank for International Settlements (2020) The Basel Committee on Banking Supervision – overview. https://www.bis.org/bcbs/index.htm.

Commission (2020) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU.

Commission (2020) Proposal for a Regulation of The Euro- pean Parliament and of the Council on contestable and fair markets in the digital sector.

Commission (2021) Summary - Consultation on a new Digital Finance strategy.

Commission. Communication from The Commission To The European Parliament And The Council New Consumer Agenda Strengthening Consumer Resilience For Sustainable Recovery Com/2020/696 Final.

Commission. Communication from the Commission to The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions A European Consumer Agenda - Boosting Confidence And Growth /Com/2012/0225 Final.

Commission. Communication From The Commission To The European Parliament And The Council New Consumer Agenda Strengthening Consumer Resilience For Sustainable Recovery Com/2020/696 Final (New Consumer Agenda).

Commission. Legislative proposal for an EU framework on crowd and peer to peer finance. COM (2018)113.

Committee of European Securities Regulators (2010), Technical Advice to the European Commission in the context of the MiFID-Review and Responses to the European Commission Request for Additional Information. https://www.esma.europa.eu/document/cesr-technical-advice-european-commission-in-context-mifid-review-and-responses-european.

European Banking Authority (2019) Report with advice for the European Commission on crypto-assets.

European Banking Federation (2020) Data usage, access & sharing in the digital economy. https://www.ebf.eu/wp-content/uploads/2020/02/Data-economy-EBF-position-paper-Jan-2020.pdf.

European Commission (2008) Your questions on MiFID. https://ec.europa.eu/internal_market/securities/isd/questions/index_en.htm.

European Commission (2020) The European Blockchain Partnership'. https://ec.europa.eu/digital-single-market/en/blockchain-technologies.

European Parliament (2019) Parliamentary question n. E-002268/2019. http://www.europarl.europa.eu/doceo/document/E-9-2019-002268-ASW_EN.html.

European Parliament. Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content. COM/2015/0634 final - 2015/0287 (COD).

European Parliament. Proposal for a regulation of the European Parliament and of the Council on European crowdfunding services providers (ECSP) for Business, COM(2018) 0113 final.

European Securities and Market Authority (2014) 'Opinion on Investment based crowdfunding. https://www.esma.europa.eu/search/site/Opinion%2520investment-based%2520crowdfunding?within doc=1&solrsort=&perpage=20.

European Securities and Markets Authority (2015), Regulatory technical and implementing standards. https://www.esma.europa.eu/sites/default/files/library/2015/11/2015-esma-1464_annex_i-draft_rts_and_its_on_mifid_ii_and_mifir.pdf, Annex I MiFID II / MiFIR.

European Securities and Markets Authority (2018) Final Report: Technical advice under the Prospectus Regulation. https://www.esma.europa.eu/documenttechnical-advice-under-prospectus-regulation.

European Securities and Markets Authority (2019) Advice on Initial Coin Offerings and Crypto-Assets.

European Securities and Markets Authority (2019) Prospectuses. Questions and Answers, 29th updated version. https://www.esma.europa.eu/sites/default/files/library/esma31-62-780_qa_on_prospectus_related_topics.pdf.

Financial Action Task Force (2012) International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

Financial Conduct Authority (2019) Guidance on Cryptoassets. Feedback and Final Guidance to CP 19/3, Policy Statement PS19/22. https://www.fca.org.uk/publication/policy/ps19-22.pdf.

Financial Conduct Authority (2019), Chapter 13: Guidance on the scope of MiFID and CRD IV, *FCA*, https://www.handbook.fca.org.uk/handbook/PERG/13.pdf.

Financial Crimes Enforcement Network (FinCEN) (2019) Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001. https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models.

Financial Intelligence Group (2017) From Suspicion to Action, Converting financial intelligence into greater operational impact.

Financial Stability Board (2017). Monitoring of FinTech.

Organisation for Economic Co-operation and Development (2019) 'Initial Coin Offerings (ICOs) for SME Financing', *OECD*, https://www.oecd.org/finance/initial-coin-offerings-for-sme-financing.htm.

Organisation for Economic Co-operation and Development (2020) Personal Data Use in Financial Services and the Role of Financial Education: A Consumer Centric Analysis. www.oecd.org/daf/fin/financial-education/Personal-Data-Use-in-Financial-Services-andthe-Role-of-Financial-Education.pdf.

Panel for the Future of Science and Technology (2021) Online platforms: Economic and societal effects. https://www.europarl.europa.eu/stoa/en/document/ EPRS_STU(2021)656336.

Private Equity Forum (2018). Brief insights from PEF research. N26: the rise of a fintech. https://pef-jlu.de/wp-content/uploads/2018/10/heyden_poppelreuter_2018_brief_insights_n26.pdf.

The Dutch Banking Association (2019). The case for further reform of the EU's AML framework. Report: https://www.nvb.nl/media/3002/dutch-banking-association_the-case-for-further-reform-of-the-eus-aml-framework.pdf.

The European Blockchain Observatory and Forum, https://www.eublockchainforum.eu.

The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 U.S.C. 5311 et seq.).

The International Association for Trusted Blockchain Applications, https://inatba.org.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act).

WP29 (2014) (n 85) recalling WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under art 7 of Directive 95/46/EC.

WP29 (2016) Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679.

Mastercard Global Privacy Notice. https://www.mastercard.us/en-us/vision/corp-responsibility/commitment-to-privacy/privacy.html#dataTransfer.

N26 Privacy Policy. https://docs.n26.com/legal/06+EU/03+Privacy%20Policy/en/01privacy-policy-en.pdf.

Revolut Privacy Policy. https://www.revolut.com/legal/privacy.

PayPal User Corporate rules. https://www.paypalobjects.com/marketing/ua/pdf/GB/en/bcr.pdf.

Visa Global Privacy Notice. https://www.visa.co.uk/legal/global-privacy-notice.html.

CASE LAW

SEC, *In the Matter of Munchee Inc.,* Order (2017).
SEC v. W.J. Howey Co., 328 U.S. 293 (1946).
CONSOB, delibera n. 20740/2018
CONSOB, delibera n. 20741/2018.
NJCM et al. and FNV v The State Of The Netherlands [2020], ECLI:NL: RBDHA:2020:865.

SUMMARY

This manuscript is a journey through coexisting, emerging or speculated about, types of digital value transfer infrastructures. Using digital value transfer infrastructures as a central case study, this thesis is concerned with unpacking the negotiation processes that shape the governance, design and political purposes of digital infrastructures that are closely linked to the public interest and state sovereignty. In particular, the papers that are assembled in this manuscript identify and inspect three main socio-technical developments occurring in the domain of value transfer technologies: a) the privatization and platformization of digital payment infrastructures; b) the spread of blockchain-based digital value transfer infrastructures; c) the construction of digital value transfer infrastructures as public utilities, from the part of public institutions or organizations. Concerned with the relationship between law, discourse and technological development, the thesis explores four transversal issues that strike differences and peculiarities of these three scenarios: i) privacy; ii) the synergy and mutual influence of legal change and technological development in the construction of digital infrastructures; iii) the role of socio-technical imaginaries in policy-making concerned with digital infrastructures; iv) the geography and scale of digital infrastructures.

Chapter 1 presents the conceptual scaffoldings upon which the research is developed. It introduces the concept of 'infrastructure' and explains how this manuscript uses it as an analytical tool. The introductory chapter also provides definitions of terms - such as "value transfer infrastructure", "money", "platform" and "blockchain-based digital currencies" – that are necessary for understanding the use cases presented in the thesis. Chapter 1 also introduces

the research questions, it grounds them on the theoretical background, and it presents the research methods deployed to answer them.

Highlighting the most critical trends of the current financial industry (i.e. commercial exploitation of data; international dimension of financial informational networks; use of automated processing and decision-making tools), Chapter 2 analyses how privacy and law enforcement priorities interplay in determining the governance of financial data. It concludes by recognizing that privacy loop-holes exist in the current financial industry's data practices, and that - as payments tend to be increasingly performed in digital manners, exponentially increasing the availability of financial data - privacy-enhancing payment methods should be encouraged and legitimised.

Staring from an analysis of the guidelines issued by the European Securities and Market Authority and by the European Banking Authority, Chapter 3 discusses the legal qualification of blockchain-based crypto-assets. Hence, it outlines shortages and drawbacks in the applicability and enforcement of existing EU legal frameworks. The conclusion elaborates on the relationship between law enforcement, regulatory intervention and socio-technical developments in the crypto-assets ecosystem.

Chapter 4 investigates, through a qualitative analysis of official documents, how certain imaginaries about technology filter into EU policymaking, allowing or accelerating the trans- formation of payment infrastructures into the platform economy. One of the ways in which socio-technical imaginaries filter into policymaking is, it turns out, by informing an image of the consumer which serves to justify measures for the realization of a desired future. The thesis proposed with this chapter is that this view of the consumer is partial: the rhetoric of consumer technological empowerment outweighs and conceals much needed considerations about the vulnerability of consumers vis-á-vis data-intensive payment technologies. Therefore, the conclusion suggests that policymakers should be more critical of the risks entailed by platformization, and open their imagination to alternative technological futures.

Chapter 5 is concerned with investigating the relationship between scale, socio-political goals and technological design of digital money infrastructures. Using interviews, the chapter explores three publicly-founded projects

that organize digital money infrastructures at different scales. By comparing the latter, it emerges that smaller scale and bottom-up governance equals to higher attention to local problems and social dynamics; however, links to institutions and top-down decision-making seem to be better able to realize long-lasting and scalable digital money infrastructures.

Chapter 6 draws the general conclusions. Grounding the criticism of the legal construction of privacy on the political economy of the actors that organize digital commerce and information flows, the conclusions of this manuscript invite academics and regulators to widen their imagination to alternative possible futures of digital infrastructures. It advocates the acceptance of imperfection as opposed to 'perfect targeting' and 'perfect enforcement'. It welcomes the rise of multiple, contested, delocalized and vertically overlapping digital value transfer infrastructures, as they express the prerogatives of different groups – social, economic and political actors. It suggests, ultimately, that plurality is a necessary antidote against the totalizing effects of surveillance apparatuses enabled by datafication and algorithmic enforcement. It argues that the possibility of an "outside" in the landscape of possible digital architectures needs to remain imaginable and designable. For this reason, in the co-development of legal systems and digital infrastructures that are core to public life, conflicts are productive. Negotiations, ruptures and exceptions are constitutive of the unending process of mutual reinforcement, and mutual containment, in which a plurality of agencies – expressed through legal institutions, symbolic systems, as well as information and media structures - are entangled.

SAMENVATTING

Dit manuscript is een reis door naast elkaar bestaande, opkomende of gespeculeerde soorten infrastructuren voor digitale waardeoverdracht. Met behulp van infrastructuren voor digitale waardeoverdracht als centrale casestudy, gaat dit proefschrift over het ontrafelen van de onderhandelingsprocessen die vorm geven aan het bestuur, het ontwerp en de politieke doeleinden van digitale infrastructuren die nauw verbonden zijn met het algemeen belang en de soevereiniteit van de staat. In het bijzonder identificeren en inspecteren de papers die in dit manuscript zijn verzameld drie belangrijke sociaal-technische ontwikkelingen die plaatsvinden op het gebied van technologieën voor waardeoverdracht: a) de privatisering en platformisering van digitale betalingsinfrastructuren; b) de verspreiding van op blockchain gebaseerde infrastructuren voor digitale waardeoverdracht; c) de aanleg van infrastructuren voor digitale waardeoverdracht als openbare voorzieningen, van de kant van openbare instellingen of organisaties. Bezorgd over de relatie tussen recht, discours en technologische ontwikkeling, onderzoekt dit proefschrift vier transversale kwesties die de verschillen en eigenaardigheden van deze drie scenario's opmerken: i) privacy; ii) de synergie en wederzijdse beïnvloeding van juridische verandering en technologische ontwikkeling bij de aanleg van digitale infrastructuren; iii) de rol van socio-technische denkbeelden in de beleidsvorming met betrekking tot digitale infrastructuren; iv) de geografie en schaal van digitale infrastructuren.

Hoofdstuk 1 presenteert de conceptuele onderbouwingen waarop het onderzoek is ontwikkeld. Het introduceert het concept 'infrastructuur' en legt uit hoe dit manuscript het gebruikt als analytisch instrument. Het

inleidende hoofdstuk geeft ook definities van termen - zoals "infrastructuur voor waardeoverdracht", "geld", "platform" en "op blockchain gebaseerde digitale valuta's" - die nodig zijn om de in dit proefschrift gepresenteerde use cases te begrijpen. Hoofdstuk 1 introduceert ook de onderzoeksvragen, baseert ze op de theoretische achtergrond en presenteert de onderzoeksmethoden die zijn gebruikt om ze te beantwoorden.

In hoofdstuk 2 worden de belangrijkste trends van de huidige financiële sector (d.w.z. commerciële exploitatie van gegevens; internationale dimensie van financiële informatienetwerken; gebruik van geautomatiseerde verwerkings- en besluitvormingsinstrumenten) belicht. financiële data. Het concludeert door te erkennen dat er mazen in de privacywetgeving bestaan in de gegevenspraktijken van de huidige financiële sector, en dat - aangezien betalingen steeds vaker op digitale manieren worden uitgevoerd, waardoor de beschikbaarheid van financiële gegevens exponentieel toeneemt - privacybevorderende betalingsmethoden moeten worden aangemoedigd en gelegitimeerd .

Uitgaand van een analyse van de richtlijnen van de European Securities and Market Authority en de European Banking Authority, bespreekt hoofdstuk 3 de juridische kwalificatie van blockchain-gebaseerde crypto-assets. Daarom schetst het tekorten en nadelen in de toepasbaarheid en handhaving van bestaande EU-rechtskaders. De conclusie gaat dieper in op de relatie tussen wetshandhaving, regelgevende interventie en sociaal-technische ontwikkelingen in het crypto-activa-ecosysteem.

Hoofdstuk 4 onderzoekt, door middel van een kwalitatieve analyse van officiële documenten, hoe bepaalde denkbeelden over technologie doorsijpelen in de EU-beleidsvorming, waardoor de transformatie van betalingsinfrastructuren naar de platformeconomie mogelijk wordt gemaakt of versneld. Een van de manieren waarop socio-technische verbeeldingen doorsijpelen in de beleidsvorming, zo blijkt, is door een beeld van de consument te informeren dat dient om maatregelen voor de realisatie van een gewenste toekomst te rechtvaardigen. De stelling die in dit hoofdstuk wordt voorgesteld, is dat deze kijk op de consument partieel is: de retoriek van technologische empowerment van de consument weegt zwaarder dan en verbergt broodnodige overwegingen over de kwetsbaarheid van consumenten ten opzichte

van data-intensieve betalingstechnologieën. Daarom suggereert de conclusie dat beleidsmakers kritischer moeten zijn over de risico's die platformisering met zich meebrengt, en hun verbeelding moeten openen voor alternatieve technologische toekomsten.

Hoofdstuk 5 gaat over het onderzoeken van de relatie tussen schaal, sociaal-politieke doelen en technologisch ontwerp van digitale geldinfrastructuren. Aan de hand van interviews onderzoekt het hoofdstuk drie publiekelijk gefundeerde projecten die digitale geldinfrastructuren op verschillende schaalniveaus organiseren. Door de laatste te vergelijken, blijkt dat kleinschaliger en bottom-up bestuur gelijk staat aan meer aandacht voor lokale problemen en sociale dynamiek; koppelingen met instituties en top-down besluitvorming lijken echter beter in staat om duurzame en schaalbare digitale geldinfrastructuren te realiseren.

Hoofdstuk 6 trekt de algemene conclusies. De conclusies van dit manuscript baseren de kritiek op de juridische constructie van privacy op de politieke economie van de actoren die digitale handel en informatiestromen organiseren, en nodigen academici en regelgevers uit om hun verbeeldingskracht te verbreden naar alternatieve mogelijke toekomsten van digitale infrastructuren. Het pleit voor de acceptatie van imperfectie in tegenstelling tot 'perfecte targeting' en 'perfecte handhaving'. Het verwelkomt de opkomst van meerdere, omstreden, gedelokaliseerde en verticaal overlappende infrastructuren voor digitale waardeoverdracht, aangezien deze de prerogatieven van verschillende groepen - sociale, economische en politieke actoren - tot uitdrukking brengen. Het suggereert uiteindelijk dat pluraliteit een noodzakelijk tegengif is tegen de totaliserende effecten van bewakingsapparaten die mogelijk worden gemaakt door dataficatie en algoritmische handhaving. Het betoogt dat de mogelijkheid van een "buiten" in het landschap van mogelijke digitale architecturen denkbaar en ontwerpbaar moet blijven. Om deze reden zijn conflicten productief in de gezamenlijke ontwikkeling van rechtsstelsels en digitale infrastructuren die de kern vormen van het openbare leven. Onderhandelingen, breuken en uitzonderingen zijn constitutief voor het eindeloze proces van wederzijdse versterking en wederzijdse inperking, waarin een veelheid aan agentschappen - uitgedrukt door juridische instellingen, symbolische systemen, evenals informatie- en mediastructuren - verstrikt raakt.

ACKNOWLEDGEMENTS

But when the web is pulled askew, hooked up at the edge, torn in the middle, one remembers that these webs are not spun in mid-air by incorporeal creatures, but are the work of suffering human beings, and are attached to grossly material things, like health and money and the houses we live in.
VIRGINIA WOOLF, *A Room of One's Own*

Well sometimes I think that I'm bigger than the sound.
YEAH YEAH YEAHS

What I find most stupefying about this manuscript is how well its academic, technical style of writing conceals and levels out the wide spectrum of emotions that accompanied its materialization. Anyone who was there during the journey knows how much I wrestled with these pages, struggling to give a direction to my curiosity, to reconcile that curiosity with the expectations of the institutions and of the people around me. Thankfully, endings can be resolutive, and now I can look at those moments of struggle with appreciation, with self-respect, and most of all, with gratitude, because it is thanks to the support of wonderful friends, colleagues, and comrades that I have completed the journey.

I started my Ph.D. knowing very little about what it means to be in academia. I wasn't even aware, when I was hired, of how much of a privilege it was to be part of the Institute of Information Law (IViR) – a privilege and a challenge. Most of the other Ph.D. students at the institute were Dutch and had completed the IViR research master program. I could have

felt discouraged, intimidated, and unfit. However, I didn't: from the start of my Ph.D., I found belonging and solidarity within my research group, the Blockchain and Society Policy and Research Lab, and within the whole institute.

The feeling of privilege came, first of all, from the material conditions in which I found myself working. My first expression of gratitude goes to Anja Dobbelsteen, Margriet Pauws-Huisink, the cleaning staff, and all the people at UvA who put their efforts into creating the environment for me and for the other researchers to work comfortably. Then, I obviously need to thank my mentor, Balázs Bodó. Our relationship has been, I believe, as complex and valuable as it can get. With a lot of suffered "unpack" and "explain", he pulled me out of my intellectual comfort zones, squeezing more thinking out of my writing. I now feel extremely grateful for all the headaches he gave me, for teaching me how to use my knowledge and my language in ways I didn't think I would be capable of.

Some higher will, astrological alignment, or simply luck wanted Balázs to hire, at the same time and for the same project he hired me, Alexandra Giannopoulou. I don't know how I would have survived Amsterdam, UvA, and each and every academic conference I went to, without her. Alex hasn't only been my colleague, but also my closest friend, my mum, my sister, my party buddy, and my emotional support in the best and worst moments of these past four (five?) years. I hope she already knows how grateful I am for her existence; I hope she felt this gratitude at each of the steps she helped me overcome.

I was one and a half year into my Ph.D. when Covid-19 arrived. The pandemic forced me home, working in isolation, getting bored. That period taught me many things; first and foremost, it made me appreciate the invaluable luck of being surrounded by smart, funny, respectful, and supportive colleagues. João Quintais's levity and humor have been the best antidotes to alienation at the UvA offices. Heleen Janssen's kindness is such a precious asset; I have been truly glad to have her in our team. The entire Young IViR squad – Jill Toh, Naomi Appelman, Jef Ausloos, Marijn Sax, Max van Drunen, Ronan Fahy, Ljubiša Metikoš, Paddy Leerssen, and all the others – has been life-saving with its nerdy academic jokes that helped us exorcise shared trauma. My gratitude also goes to the smiley faces that made UvA a friendly place:

Marija Bartl, Alessio Pacces, and Edoardo Martino. To Kristina Irion for her exemplary strength. To all the past and future students of the Law as a Change Maker course, for their enthusiasm.

I am grateful to all my many supervisors. Nico Van Eijk, who first welcomed me at the institute and who I think would have been a perfect match for my temperament. Martin Senftleben and Joost Poort, who jumped in last minute to save my career, putting faith in my work and providing precious feedback so I could finalize my dissertation. Egbert Dommering, for his invaluable lessons about power, and knowledge; he taught me how to better handle the first, and sparked ideas in me about how to use the second in the future.

Companionship is crucial to survival in the academic world. I probably would have given up writing if it wasn't for the encouragement and support of my comrades: Gianmarco Cristofari, who initiated an international platform of friendship; Letizia Chiappini, forever my academic bestie, companion of daydreaming and sluttiness; Tommaso Campagna, whose hugs have been the crucial "technical" support to my work; Giovanni Rossetti, for the real and imagined afternoons at the library; Ying-Tzu Lin (Connie), for her cynical humor and for simply knowing better; Davide Beraldo, for being the academic we one day want to be; Anastasia Dolitsay (Ray), for overdressing our days; Geert Lovink and all the beautiful people at the Institute of Network Cultures, for making me feel welcome; and of course Jordi Viader Guerrero (my princess husband), for so brilliantly deciphering my intellectual and emotional intricacies, and helping me organize them.

When I think about this period in Amsterdam, I will remember, certainly with amazement, all the beautiful, creative minds that enriched my journey with unexpected discoveries. Jean Medina – our friendship started at a café chatting about Borges, and I hope it will continue influencing our respective libraries; Jana Petkanic, you managed to transform me into an entrepreneur, and to almost make me love math. Aron Fischer, every encounter with you was a learning experience.

I also need to thank all the people who have dealt with my stress, my chaos, my euphoria, and my madness in the houses I have lived in during these troubled years: Alessandro Amarri and Gregorio Villirillo (the Tutucu family)

will always be synonymous with “home”; Damian Borovsky, my partner in crime during the lockdown; and Marc and Jaime, jazzing the final months of my Ph.D.

There are a lot more people I should thank for being there throughout these years: Joyce, David, Katya, Gautham, Omer, Marianna, Dolc – I felt your love. Claudia R, you are a warrior and an amazing friend. My friends from Reggio – Ric, Cerio, Mathi, Mat, Leo, Berta, Fé, l’Anna Matilde, Esther, Bree, Cate – who keep being my gravitational center while I wander around the world. Andy Díaz Sánchez, who, among other things, I have to credit for making the printed copy of this book so guay.

Finally, I want to thank my family: Nonna, Ivano, Claudio, Fedi, Sean, Jey, Jaco, l’invincible Andry e l’incontestabile Stefano. Last but not the least, my amazing mum Francesca, who is always by my side, and – let’s be honest – made all of this (all of me) possible.