EU Supervisory
Digital Finance
Academy

Digital Finance in the EU: drivers, risks, opportunities

Editors

Thorsten Beck, Leonardo Giani, Giuseppe Sciascia

Funded by
the European Union

European Commission

EUI EUROPEAN UNIVERSITY INSTITUTE

eba European Banking Authority

eiopa EUROPEAN INSURANCE

ESMA European Securities and Markets Authority

Views expressed in this publication reflect the opinion of individual authors and not those of the European University Institute.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

This e-book has received funding from the EU TSI Programme in the framework of the EU Supervisory Digital Finance Academy (EU-SDFA) project, grant agreement number 101092497.

Published by
European University Institute (EUI)
Via dei Roccettini 9, I-50014
San Domenico di Fiesole (FI)
Italy

ISBN:978-92-9466-490-7
doi:10.2870/51343
QN:QM-02-23-285-EN-N

Funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.
This e-book has received funding from the EU TSI Programme in the framework of EU-SDFA project, grant agreement number 101092497

Digital Finance in the EU: drivers, risks, opportunities

The EU Supervisory Digital Finance Academy's First Year e-Book

EDITED BY
Thorsten Beck, Leonardo Giani, Giuseppe Sciascia

European University Institute, Florence, Italy

Table of Contents

Section 1

1. Foreword 7
Mario Nava

2. Introduction 10
Thorsten Beck, Leonardo Giani, Giuseppe Sciascia

3. The state of digital finance in Europe 14
Alice Guedel, Giuseppe Sciascia

4. Digital finance in the global context: Challenges and perspectives 26
Ignazio Angeloni

Section 2

1. Blockchain and DeFi – An economist's perspective for supervisors 40
Thorsten Koeppl

2. Safe AI & ML 49
Paolo Giudici

3. Artificial intelligence and machine learning in the hearts of central banks and supervisors: A case study of the Dutch central bank 61
Patty Duijm, Iman van Lelyveld

4. Sandboxes and financial innovation facilitators 77
Alain Otaegui Chapartegui

Section 3

1. Cyber risk and the financial sector 91
Emran Islam, Klaus Löber

2. Fintech and green fintech –
Digital innovation for the SDGs and climate agenda 105
Katherine Foster

3. SupTech 120
Claudia Guagliano, Valentina Mejdahl

4. RegTech 134
Maha Abbassi

5. Analysing digital business models 146
Adrian Mora-Moreno

6. Selected case studies 156
Maha Abbassi, Giulio Bagattini, Andres Lehtmets

Section 1

Introduction and overview

1. Foreword

Mario Nava

Director General for Structural Reform Support - European Commission

In the last two decades the world has witnessed an extraordinary technology-driven change in the financial system with unprecedented effects that are still far from being overcome. While technological innovation has always been part and parcel of finance, the disruption brought by the application of innovative technologies to various financial flows has projected regulatory and supervisory authorities into a new era. Digital finance is becoming ever less a niche trend. Instead, it is a truly ubiquitous phenomenon pervading the lives of billions of people around the world. Capturing the opportunities it offers and managing its potential risks represent key challenges for regulatory and supervisory authorities within and beyond the EU.

This e-book is the result of the first year of implementation of an ambitious and far-reaching technical support project launched by the European Commission (DG REFORM) in October 2022:[1] the EU Supervisory Digital Finance Academy (EU-SDFA). Until 2025, and possibly beyond, the Academy will bring together experts from Member State financial supervisory authorities with a view to developing their skills and capacity in relation to the application of advanced technologies to financial services, products and markets. The EU-SDFA is a unique cross-sectoral EU-wide initiative aimed at overcoming sectoral barriers, fostering a common culture and understanding of digital

[1] The mission of DG REFORM is to provide Member States with tailor-made technical support leveraging the resources of the Technical Support Instrument – the European Commission's key tool to support the design and implementation of inclusive growth-enhancing reforms. DG REFORM covers a broad range of policy areas, from public administration transformation to labour, health, energy and the financial sector. It mobilises resources to provide Member States with result-oriented support, cooperating with international organisations and public and private sector experts.

finance issues in order to build an inclusive community of financial sector experts able to manage the disruptive challenges brought by digitalisation.

The journey leading to the launch of the EU-SDFA started back in 2020. In the midst of the third wave of the Covid-19 pandemic we started to reflect on how best to support the Member States in coping with the significant multiple challenges faced by the economy. Digitalisation, with its pervasive effects, clearly appeared a topic too big to ignore – and all the more in the financial sector. The EU-SDFA was presented as the first flagship project for the financial sector in the Technical Support Instrument (TSI) 2022 cycle, and as a concrete opportunity for the Member States to effectively match the pressing demand for a profound revamp of supervisory skills and knowledge in the area of digital finance. Therefore, the EU-SDFA addresses a cross-cutting need by exploiting economies of scale and adding an EU-wide perspective and a cross-sectoral dimension, building on the objectives of the Digital Financial Strategy adopted in September 2020.

The EU-SDFA's comprehensive and diversified learning path is complemented by activities that help develop practical skills, enable exchanges and knowledge-sharing on cutting-edge issues, and effectively promote the establishment of a community of digital-savvy supervisors fully equipped to face the challenges brought by the disruption caused by digital finance and drive change in the regulatory and supervisory world. We are confident that the Academy can act as both a real multiplier and an enabler of further development. It will facilitate the sharing of knowledge, expertise and skills among the institutions participating, possibly giving rise to a flow of new actions and cooperation among the authorities. At the same time, the EU-SDFA can become an incubator of new solutions and ideas to be further developed with the European Commission's technical support as multi-country or cross-sectoral projects.

The name we have chosen for this project clearly reflects its ambitions and conceptual background. In ancient Greece, the Academy was the legendary sacred place in the surroundings of Athens where the hero Akademos was buried, and where Plato founded his school for prominent leaders and thinkers. Building on this legacy, 'academy' is now a reference term for high-level educational institutions in which learning is transferred and developed among and by the participants, helping to build a unique community of experts in a given field. The EU-SDFA has potential to become a powerful knowledge hub with multiple spokes across the EU. These spokes may be institution-specific, country-based, sectoral or cross-sectoral, enabling experts to work together beyond national borders on the basis of a common cultural background and knowledge.

DG REFORM started this project with the full support of DG FISMA and working in close partnership with the three European Supervisory Authorities (ESAs). Their collaboration and contribution are key: first, as the project complements the extensive ongoing work carried out by the ESAs themselves in the area of digital finance; second, as the ESAs bring an effective EU-wide perspective to the challenges brought by digitalisation, fostering cross-border, cross-sectoral cooperation and coordination; and third, as the project aims to ensure a positive continuous feedback loop between the build-up of knowledge and skills, and enhancement of the composite multi-layer regulatory framework to which the ESAs largely contribute.

The European University Institute Florence School of Banking and Finance is an invaluable partner in the implementation of the project. The Institute has recognised academic expertise in the area of financial regulation, and strong historical ties with the EU institutions and agencies, and a number of Member States.

The preparedness and enthusiasm of all the project partners has allowed us to successfully complete the first academic cycle and to create a solid base for the continuation of this endeavour, which will contribute to building a more resilient and innovative financial system for the benefit of EU citizens and businesses.

2. Introduction

Thorsten Beck
Professor of Financial Stability and Director of the Florence School of Banking and Finance at Robert Schuman Centre - European University Institute

Leonardo Giani
Research Fellow of the Florence School of Banking and Finance at Robert Schuman Centre - European University Institute

Giuseppe Sciascia
Policy Officer at European Commission DG for Structural Reform Support - REFORM

This e-book is published about a year after the launch of the EU Supervisory Digital Finance Academy (EU-SDFA). It contains contributions on some of the main topics covered in the training activities which took place during the first academic year of the EU-SDFA, either at the European University Institute (EUI) or in workshops hosted by the European Supervisory Authorities (ESAs).

The contributions are mainly authored by the training activity instructors. More precisely, the e-book consists of twelve contributions from different authors grouped in three broad areas. The e-book format is intended to enable past and future EU-SDFA participants to complement their learning experiences, while also providing valuable documents to rely on in the future. Indeed, although they started with teaching materials, the authors have not done a mere stock-taking exercise of the resources employed in the training sessions. They have substantially reworked and enhanced their materials, turning them into true and proper (albeit short) chapters. As such, the e-book also provides the EU-SDFA with visibility in the research and policy community by allowing experts and academics to contribute to the public debate.

Following the foreword and this introduction, the first section aims to provide an overview of the subject matter of the e-book. It starts with a contribution by Alice Guedel and Giuseppe Sciascia, who provide an outline of some of the main initiatives taken at the European Union level in the field of digital finance. In doing so, the authors consider the objectives and results to date of these initiatives, and their legacy for the future. Next, Ignazio Angeloni explores the challenges and perspectives of digital finance from a broader (i.e. global) viewpoint. His contribution starts by going back to the origins of digital finance, explaining how the concept is less new than it appears, before going into some of the most important manifestations of digital finance nowadays: cryptocurrencies; stablecoins; crypto-platforms; online payment platforms and smartphone applications; and central bank digital currencies (CBDCs). In doing so, it considers in particular their potential contributions to a more diversified, effective and efficient financial sector, possible risks and how to deal with them.

The second section considers some of the main technologies and drivers of digital finance. First, a contribution by Thorsten Koeppl describes blockchain and DeFi, outlining the current trends and challenges for supervisors. In doing so, among other things, Koeppl emphasises the essential role of trust in financial markets. The following two contributions focus on artificial intelligence (AI) and machine learning (ML). A contribution by Paolo Giudici explains how modern data-driven AI enabled by powerful ML is rapidly changing financial services leading to widespread diffusion of financial technologies. This contribution highlights the main risks and problems of financial technologies and illustrates the S.A.F.E. (Sustainable, Accurate, Fair and Explainable) model along with its policy implications. A contribution by Patty Duijm and Iman van Lelyveld discusses how to leverage the potential of data science, AI and ML based on the experiences and use cases of one central bank and supervisor: DNB (i.e. the Dutch central bank). The authors demonstrate the huge potential of data science in seven lessons. Finally, a contribution by Alain Otaegui Chapartegui provides an overview of financial innovation facilitators in the EU and describes a cross-border testing framework for the EU financial sector and new types of approaches and tools in financial innovation facilitators. It then focuses on financial innovation facilitation in specific areas of the financial sector and concludes with an outlook for innovation facilitators in the EU financial sector.

The third section focuses on the main risks and opportunities involved in digital finance. The opening contribution in this section by Emran Islam and Klaus Löber sheds light on the crucial topic of cyber risk and the financial sector. The authors suggest there are six major building blocks that, if created, could considerably reduce cyber risk and help safeguard global financial stability. They conclude that tackling cyber risk requires a coordinated approach built on a holistic strategy, effective regulation and supervision, financial stability analysis, response and recovery, information-sharing and cyber deterrence. All these require close coordination and collaboration between the authorities and the financial industry. A contribution by Katherine Foster then delves into the evolution of the sustainable development goals (SDGs) and the climate risk agenda, and focuses on the promise and challenges of digital technology in advancing these global goals. It offers definitions of some key concepts in digital finance, highlighting their significance in the context of climate risk and the SDGs, together with the challenges they bring. The contribution addresses the need for integrative approaches, pathways and governance to foster integrative inclusive sustainable financial practices and investments in climate risk mitigation and SDG solutions.

The third section continues with three contributions by experts employed by the ESAs which focus on the topics of the workshops they each hosted in the context of the EU-SDFA. A contribution by Claudia Guagliano and Valentina Mejdahl from the European Securities and Markets Authority (ESMA) deals with SupTech, starting with a definition of SupTech and an analysis of how this concept emerged and evolved in the context of financial services, explaining how the ESAs have adopted and promoted SupTech tools and concluding with a description of the benefits and challenges brought by NLP-based tools adopted by ESMA in some analytical projects. A contribution by Maha Abbassi from the European Banking Authority (EBA) focuses on RegTech. It also starts with a definition, and then outlines some examples of RegTech applications and the associated risks, to conclude with an analysis of the challenges involved and how to overcome them. A contribution by Adrian Mora-Moreno from the European Insurance and Occupational Pensions Authority (EIOPA) starts by introducing the concept of business models and puts particular emphasis on the increasing influence of digitalisation on business models in the financial sector. It then analyses the role that supervision of business models plays, especially in the context of the evolving digital landscape. Finally, it presents work carried out in this field by the ESAs to support the efforts of national competent authorities (NCAs).

The e-book concludes with a contribution written jointly by Giulio Bagattini from ESMA, Andres Lehtmets from EIOPA and Maha Abbassi from EBA which presents three selected use cases from ESMA's workshop on SupTech, EIOPA's workshop on Digital Business Model Analysis and the EBA's workshop on RegTech.

3. The state of digital finance in Europe[1]

Alice Guedel
Policy Officer at European Commission DG for Financial Stability, Financial Services and Capital Markets Union - FISMA

Giuseppe Sciascia
Policy Officer at European Commission DG for Structural Reform Support - REFORM

1. Introduction

Over the last decade, innovative technologies such as artificial intelligence (AI), machine learning (ML), distributed ledger technologies (DLT), big data and cloud computing have been significantly transforming the financial system, giving rise to new products, services, applications, processes, and business models. Generally referred to as 'digital finance,' this phenomenon benefits financial market participants and users, including financial institutions, consumers, companies, and supervisory authorities. Indeed, it enables greater and more inclusive access to financial services, wider product choice, a more competitive landscape and increased operational efficiency. Flowing investments prompted by efforts towards the digital transition prompt continual progress, as is shown by recent developments in generative AI and open finance.

Along with the advantages and opportunities, digital finance has been

[1] The views expressed here are those of the authors and do not necessarily reflect those of the European Commission.

raising new risks and challenges, which regulatory and supervisory authorities around the world have started to monitor, assess, and mitigate. Digital finance creates risks of heightened fraud, volatility and losses for investors and consumers. Increased reliance on IT and data infrastructure exposes the whole financial sector and individual institutions to increased vulnerabilities, including cyber threats, disastrous data losses and heavy reliance on third party services. The growing use of big data collected from various sources, stored, and then elaborated using AI-based applications, may give rise to financial exclusion, discriminatory practices and biases, ultimately affecting consumer outcomes.

To govern the transformative changes brought by digital finance and further pursue the ambition for a post-Covid-19 recovery that embraces the digital transition, the European Commission put forward a series of significant policymaking initiatives, setting a new pace in the global landscape of regulatory responses to the evolution of digital finance. Significant legislative actions such as rules on crypto activities and digital operational resilience have now entered into force and are gradually being phased in. More recent proposals – such as ones on the design of a digital euro and open finance – will further enrich the regulatory landscape, driving further change in the EU digital finance industry. This chapter provides a chronological overview of some of these major initiatives, focusing on their overarching objectives and results to date, and their legacy for the years to come.

2. The 2020 digital finance package: The digital finance strategy

In September 2020, the European Commission adopted a digital finance package, including a Digital Finance Strategy for the EU[2] and legislative proposals on markets for crypto-assets and digital resilience COM(2020). The Digital Finance Strategy provided the general lines on support for the digital transformation of finance in the coming years, while outlining a framework to regulate its risks. The strategy aims to link sector-specific digital finance actions to the broader context of the Commission's overarching policy goals, including a greater geopolitical and competitive role for Europe, the green transition and a deepening of capital markets. Indeed, digital finance has the potential to

[2] See EC (2020) COM(2020) 591 final. The Digital Finance Strategy for the EU sets out a general framework for how Europe can support the digital transformation of finance in the coming years, while regulating its risks.

unleash European innovation and create opportunities to develop better financial products for consumers while unlocking new ways of channelling funding to EU businesses, in particular SMEs. Therefore, its development will support the European economic recovery strategy and the broader economic transformation, opening new channels to mobilise funding in support of the Green Deal and the New Industrial Strategy for Europe. [3]

The EU's Digital Finance Strategy is centred on four main priorities: removing fragmentation in the Digital Single Market; adapting the EU regulatory framework to facilitate digital innovation; promoting data-driven innovation in finance; and addressing the challenges and risks associated with the digital transformation.

To achieve the first objective, the strategy proposes to enable EU-wide interoperable use of digital identities, to introduce passporting mechanisms and regulatory harmonisation for firms and activities with a high innovative potential and to foster cooperation through the European Forum of Innovation Facilitators (EFIF) and a new EU digital finance platform (see below). Achieving the second priority depends on putting in place a comprehensive regulatory framework enabling the uptake of DLT and crypto assets in the financial sector while mitigating their risks, along with initiatives to promote the use of AI applications and cloud computing infrastructure. The strategy also proposes establishing a common financial data space to facilitate real-time digital access to all regulated financial information, also leveraging the promotion of innovative IT tools enabling reporting and supervision, and a framework to allow B2B data-sharing (within and beyond the financial sector). The last strategic priority of addressing the challenges and risks of digital finance refers to adaptation of prudential and conduct regulation and supervision of the new financial landscape with a continual focus on consumers' interests, mitigation of AML risks, and strengthening of operational resilience for financial institutions.

3. Regulating the market in cryptos: the MiCA Regulation

Regulation of markets in crypto-assets represents one of the major milestones achieved as a follow-up to the 2020 Digital Finance Strategy. The 2020 Digital Finance Package already included a proposal for a Regulation on the Markets in Crypto-Assets (MiCA) aimed at promoting responsible innovation in cryp-

[3] See EC (2023) COM(2023) 62 final.

to-asset markets while providing heightened market integrity, consumer and investor protection, and preserving financial stability. As a result of the subsequent legislative process, MiCA officially entered into force in June 2023.[4] The Regulation includes a substantial number of Level 2 and Level 3 measures that must be developed before the fully-fledged entry into application of the new regime (within a 12-to-18-month deadline depending on the mandate).

MiCA establishes uniform EU market rules for crypto-assets. In particular, the regulation covers crypto-assets that are fungible (excluding so called non-fungible tokens due to their non-financial nature) and that are not currently regulated by existing financial services legislation.[5] Key provisions on regulated entities issuing and trading crypto-assets (including asset-reference tokens and e-money tokens) cover transparency, disclosure, authorisation and supervision of transactions. The MiCA framework hence aims to address the key risks which have appeared in recent crypto-asset market turmoil.

First, prospective purchasers and holders of crypto-assets should be informed about the characteristics, functions, and risks of crypto-assets they intend to purchase. To this end, when making a public offer of crypto-assets, or when seeking admission of crypto-assets to trading on a trading platform for crypto-assets, issuers, offerors, and persons seeking admission to trading of crypto-assets should produce, notify to their competent authority and publish an information document ('a crypto-asset white paper') containing mandatory disclosures. Second, to ensure market integrity and reduce the risks of fraud, MiCA introduces organisational, operational and prudential requirements for issuers of crypto assets and crypto asset service providers like trading venues and wallets. These requirements include establishing a clear organisational

[4] Regulation (EU) 2023/1114.

[5] MiCA has introduced particularly stringent rules for so-called stablecoins, i.e. tokens that aim to maintain a stable value in relation to an official currency, or in relation to one or several assets, via protocols, that provide for the increase or decrease in the supply of such crypto-assets in response to changes in demand. In this regard, MiCA distinguishes between i) e-money tokens (EMTs), i.e. crypto assets that purport to maintain a stable value by referencing the value of one official currency, and ii) asset-referenced tokens (ARTs), i.e. crypto-assets that are not an EMT and that purport to maintain a stable value by referencing any other value or right or a combination thereof, including one or more official currencies. EMTs can only be issued by an authorised e-money institution or credit institution, subject to notification of a white paper to the competent authority and its subsequent publication. Strict requirements apply to their marketing and redeemability, and investment of funds received in exchange for their availability. ARTs can only be issued by a credit institution or by a legal person or other undertaking established in the EU that has been authorised pursuant to MiCA itself. The Regulation details the supervisory process applicable to such issuers, and their conduct, information and risk management obligations.

structure, transparent and consistent lines of responsibility, a fit and proper management structure, risk assessment mechanisms and rules for the management of conflicts of interest. In addition, MiCA provides specific rules for the prevention of market manipulation and insider trading (market abuse), while specific rules aim at preventing hacks and bugs in the blockchain, requiring the establishment of adequate IT security procedures and systems in place to guard against cyber risks and IT failures. Finally, to ensure that risks of money laundering, terrorist financing and sanctions circumvention are mitigated, crypto asset service providers covered by MiCA are included in the list of 'obliged entities' under the AML framework. As such, they must comply with the AML/CTF regulatory framework.

4. Protecting digital operational resilience: the DORA framework

The second main legislative proposal included in the 2020 Digital Finance Package focuses on addressing the risks associated with the financial sector's growing dependence on software and digital processes. The Commission proposal aims to strengthen firms' capacity to withstand ICT-related disruptions and threats, mandating compliance with strict requirements to prevent and limit the impact of ICT-related incidents. In addition, the proposed framework outlines a mechanism to oversee service providers (such as BigTechs) which provide cloud computing services to financial institutions.

This initiative interrelates with a wider workstream ongoing at the European and international levels to strengthen cybersecurity in financial services and address broader operational risks. The proposal also responds to the 2019 Joint technical advice of the European Supervisory Authorities (ESAs), which called for a more coherent approach in addressing ICT risks in finance and recommended that the Commission should strengthen, in a proportionate way, the digital operational resilience of the financial services industry with an EU sector-specific initiative. The ESAs' advice was a response to the Commission's 2018 Fintech action plan COM(2018).

The final text of DORA was signed on 14 December 2022 and published in the EU Official Journal on 27 December 2022.[6] The DORA Regulation sets out specific requirements for the security of network and information systems of companies and organisations operating in the financial sector and of critical

[6] Regulation (EU) 2022/2554.

third parties which provide them with ICT-related services, such as cloud platforms and data analysis services. Under the new framework, financial firms will have to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats, and critical third-country ICT service providers to financial entities in the EU will be required to establish subsidiaries in the EU so that oversight can be properly implemented.

5. The digital finance platform and the data hub

As a follow-up to the launch of the 2020 Digital Finance Strategy, the Commission established a platform aimed at supporting innovation in finance and building a true single market for digital financial services. The Digital Finance Platform was created to serve long-standing requests identified by stakeholders, to develop closer relationships between innovative firms (fintechs and established financial entities) and NCAs, and to set up an entry point into the single market. The Digital Finance Platform is a collaborative space that offers practical tools designed to facilitate the scaling up of innovative firms across Member States.

In the Digital Finance Platform, the Data Hub will make specific sets of non-public non-personal data[7] available to participating firms with a view to enabling them to test innovative products and train AI/ML models. The Data Hub will therefore complement national sandboxes and innovation hubs that typically focus on facilitating dialogue between regulators and innovators for private and public sector use cases, complementing the existing Digital Finance Platform's cross-border testing features. The Hub will hence ultimately make it easier to develop products that depend on data-intensive AI systems so as to promote the competitiveness of EU firms. The initiative is part of the Data Strategy COM(2020) with which the EU commits to boosting the development of trustworthy data-sharing systems by means of four broad sets

[7] To ensure compliance with confidentiality requirements, the Commission – together with NCAs – has decided to build the data hub using synthetic data. Synthetic data offers a way for national supervisors to participate in the project without having to make the real data they hold accessible to any third party. Synthetic data would be generated from original confidential data held by the NCAs so that the real data would never leave the premises of the supervisor and no external user would access the data and the supervisor would be the legal owner of the synthetic data and would commit to make it available on the data hub. In summary, synthetic data would ensure full anonymisation while preserving the characteristics of the original data that make it relevant for testing purposes. This method makes it possible to generate synthetic data that offers the necessary level of anonymisation while preserving the characteristics of the original data that make it relevant for testing purposes.

of measures, one of which is to facilitate the reuse of public sector data that cannot be made available as open data.

6. A revised strategy for retail payments

The 2020 Retail Payments Strategy represents the second non-legislative initiative included in the 2020 Digital Finance Package. The Retail Payments Strategy for the EU aims to further develop the European payments market so the EU can fully benefit from innovation and the opportunities that come with digitalisation. The strategy focuses on creating the conditions to make the development of instant payments and EU-wide payment solutions possible, ensuring consumer protection and the safety of payment solutions, and reducing Europe's dependence on big global players in this area.

The 2020 Retail Payments Strategy contains four pillars: increasingly digital and instant payment solutions with a pan-European reach; innovative and competitive retail payment markets; efficient and interoperable retail payments systems and other support infrastructure; and more efficient international payments.

7. The framework for Financial Data Access (FIDA)

In 2020, the Commission identified the promotion of data-driven finance as one of the priorities in its Digital Finance Strategy and stated its intention to put forward a legislative proposal for an open finance framework. The Capital Markets Union Communication adopted in 2021 confirmed the Commission's ambition to accelerate its work on open finance and announced the establishment of an Expert Group on the European Financial Data Space to provide input on a first set of use cases related to open finance. President von der Leyen confirmed in her 2022 State of the Union Letter of Intent that data access in financial services is among the key new initiatives for 2023.[8]

In June 2023, the European Commission put forward a series of proposals to further improve consumer protection and competition in electronic payments, and to empower consumers to share their data in a secure way so that they can get a wider range of better and cheaper financial products and services. The initiatives proposed in the June 2023 package ultimately aimed to

[8] EC (2023).

ensure that the EU's financial sector is fit for purpose and capable of adapting to the ongoing digital transformation, and the risks and opportunities it will bring.

A first set of measures proposed in the June 2023 package include proposed amendments to modernise the Payment Services Directive (hence adoption of the PSD3) and to also establish a Payment Services Regulation.[9] Together, these will ensure consumers can continue to make electronic payments and transactions in a safe and secure manner, domestically or cross-border, in euros and other currencies. While safeguarding their rights, it also aims to provide a greater choice of payment service providers on the market.

A second set of measures is embodied in a legislative proposal for a framework for financial data access.[10] This framework will establish clear rights and obligations to manage customer data sharing in the financial sector beyond payment accounts. In practice, this will lead to more innovative financial products and services for users and will stimulate competition in the financial sector. The objective of this proposal is to promote digital transformation and speed up adoption of data-driven business models in the EU financial sector to improve economic outcomes for financial services customers (consumers and businesses) and financial sector firms. Once achieved, consumers and SMEs will be able to access individualised, data-driven financial products and services that may better fit their specific needs. Financial institutions will be able to take full advantage of digital transformation trends, while third-party service providers will develop new business opportunities through data-driven innovation. Consumers and firms will be given access to their financial data in order to enable data users (financial institutions and financial information service providers) to provide tailored financial products and services that better suit the needs of customers and firms.

The proposal leverages on the experience of the second Payment Services Directive. The PSD2 already enables the sharing of payment account data according to the 'open banking' model. This recent proposal will enable the sharing of a broader set of financial services data and sets the rules according to which sharing these data is going to be achieved and the rules applicable to the market participants who will engage in this activity.

In this respect, the proposal establishes rules in accordance with which certain categories of customer data in finance may be accessed, shared and used.

[9] See EC (2023) COM(2023) 367 final and EC (2023) COM(2023) 366 final.

[10] See EC (2023) COM(2023) 360 final.

In addition, it includes provisions concerning the transparency of conditions and information requirements for access, sharing and use of data in finance, and the rights and obligations of data users, data holders and financial information service providers. Certain safeguards geared towards consumer protection against unauthorised access and use of data are introduced. Data will only be accessed and used by authorised entities operating under a license and following the explicit consent of the consumer or business the data relates to. There are rules setting the extent to which personal data may be used, with particular attention to avoiding economic exclusion in the case the consumer does not wish to share his/her data.

8. The digital euro

In June 2023, the Commission presented the 'Single Currency Package' to support the use of cash and propose a framework for a digital euro. In the package, the Commission proposed two sets of measures to ensure that people have both payment options available when they want to pay with public money – physical and digital euros.

The first proposal aims to establish the legal framework for a possible digital euro as a complement to euro banknotes and coins, with a view to ensuring that people and businesses have another choice – in addition to the current private options – that allows them to pay digitally with a widely accepted, cheap, secure and resilient form of public money in the euro area.[11] The proposal has been put forward against the background of the European Central Bank (ECB) investigating the possibility of introducing a digital euro as a form of central bank digital currency (CBDC). It sets out the legal framework and essential elements of the digital euro,[12] which would enable the ECB to eventually introduce a digital euro that is widely usable and available, subject to further technical work.[13]

The second proposal aims to safeguard the role of cash and ensure it is widely accepted as a means of payment, hence remaining easily accessible for people and businesses across the euro area.[14] The proposed regulation lays down

[11] See EC (2023) COM(2023) 369 final.

[12] On the digital euro, see McGuinness (2023).

[13] Information on the ongoing investigation related to the introduction of the digital euro is provided by the ECB on a dedicated webpage. See here.

[14] See EC (2023) COM(2023) 364 final.

detailed rules on the scope and effects of the legal tender of, and access to, euro banknotes and coins, in order to ensure its effective use as a single currency. In this respect, the proposed regulation, among other things, i) further details the legal tender status of euro banknotes and coins, strengthening the principle of mandatory acceptance, ii) outlines cases of exceptions to this principle, having regard to refusals made in good faith and on legitimate and temporary grounds, iii) introduces obligations for EU Member States to monitor the acceptance of payments in cash and to ensure sufficient and effective access to cash throughout their territory.

9. Conclusion

Digitalisation is transforming finance for both businesses and consumers: this requires policymakers to make the most of new opportunities while managing the challenges and risks that inevitably come with them. Against this background, the Commission has prompted the adoption of a number of significant legislative and non-legislative initiatives aimed at enabling innovation, preserving market stability and integrity and protecting financial investors and consumers. Emerging business models and trends are currently being monitored by the Commission in strict coordination with the ESAs, with a view to ensuring appropriate tailoring of necessary future regulatory responses while harnessing the full potential of digital innovation applied to finance.

References

EC (2020) European Commission. *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*. COM(2020) 591 final.

EC (2023) European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A Green Deal Industrial Plan for the Net-Zero Age*. COM(2023) 62 final.

EC (2023) European Commission. *Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554*. COM(2023) 360 final.

EC (2023) European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the legal tender of euro banknotes and coins*. COM(2023) 364 final.

EC (2023) European Commission. *Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC*. COM(2023) 366 final.

EC (2023) European Commission. *Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010*. COM(2023) 367 final.

EC (2023) European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro*. COM(2023) 369 final.

EC (2023) European Commission. *State of the Union 2023, Letter of Intent*. Available here.

McGuinness M. (2023). *The case for a digital euro*. Financial Times, 28 June 2023.

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

4. Digital finance in the global context: Challenges and perspectives

Ignazio Angeloni
Part-time Professor of the Florence School of Banking and Finance at Robert Schuman Centre - European University Institute, and Senior Policy Fellow at SAFE - Goethe University Frankfurt

When dealing with technical and somewhat abused terms like 'digital finance', it is useful to stop for a moment to understand what we mean.

By digital, computer specialists denote messages coded with a sequence of binary digits, zero and one, that can be interpreted by electronic computers programmed to understand them. Finance, loosely speaking, is the set of activities involved in transforming savings (the part of national income not immediately used for personal consumption or acquisition of productive inputs) into investment (building up productive capital). Digital finance, therefore, is the part of these activities that involve the use of digital language and, by association, computers.

1. Digital finance, old and new

Seeing things in this way, one immediate observation follows: digital finance is not new at all, contrary to what most popular discourse implies. In fact, it is quite old. The first systematic use of electronic messaging to transmit payment instructions dates back to around 1918 in the United States, when the recently established Federal Reserve set up among its regional branches a payment infrastructure that went (and still goes) by the name of Fedwire. Fedwire demonstrated the miracles telecommunication can do for financial integration.[1] For the first time since US dollars were first printed some 120 years earlier, the US had a single currency with the same value all over the country. Before that, dollar values differed from one city to another depending on travel time by horse. One may argue that that technology was not digital since it did not involve binary language. That followed shortly after WWII, when Bank of America, the archetypal retail lender founded in San Francisco by the Italian immigrant Amedeo Giannini, in a joint venture with the local university (Stanford) introduced the first computerised system to manage personal cheques.[2] Its example was quickly followed by other major banks. From then on, digital finance was in full development. Cables were laid at the bottom of oceans, making digital finance global. In the 1970s, trading platforms, starting with Nasdaq, abandoned open outcry and gradually became computerised. The Depository Trust Company started offering clearing and settlement services for dematerialised securities. Shortly afterwards, computers invaded homes and offices. From the mid-1990s, they were all connected with one another through the internet.

At the turn of the century, about 90% of what we call 'money' (retail deposits at commercial banks plus bank reserves) was in digital form.[3] Nearly all the global financial system – foreign exchanges, securities and derivatives – was negotiating, trading and settling digitally. From today's perspective, the surprising thing is that all this happened without anybody paying much attention. This development seemed natural and not worth particular notice. The media did not talk about it. Politicians and regulators thought things could go on as before.

[1] See Garbade and Silber (1979).

[2] See Fischer and McKenney (1993).

[3] Around that date, broad money M3 stood close to 5,000 US$, whereas the currency in circulation was roughly one-tenth of that. Data can be found on the website of the Federal Reserve Bank of St Louis, see here.

The Great Financial Crisis changed that. The near collapse of the global financial system drew attention to the implications of the mix of finance and digitalisation for financial structures and stability. Regulators now regard digital finance as falling within their mandate. Meanwhile, the digitalisation process, far from slowing down, actually accelerated and went in new directions. Novel payment technologies and financial instruments developed at the border between the tech and financial industries. These 'new' directions constitute what most people have in mind, somewhat misleadingly, when today they talk about 'digital finance.'

Digitalisation does not change finance in a fundamental way: its inner nature and underlying risks do not change because its activities take a digital form. However, the digital support has an impact in various ways: by increasing the speed at which transactions can be executed; facilitating automation and round-the-clock activity; augmenting the possibility of diversifying and hedging risks; enhancing geographical transmission; and, more generally, requiring faster and more complex decision-making. The financial crisis of 2008-09 did not arise because of digitalisation. In essence, it was a traditional financial crisis stemming from excessive maturity transformation, lack of transparency, poor investor culture and disclosure, and overly lax regulation.[4] However, it became more global and impactful as a result of it. It is important that regulators and supervisors keep this in mind. As they immerse themselves in the fascinating and bewildering world of digital finance, they should not forget the old lessons.

Different financial compartments serve different purposes, and each has specific digital applications. Four compartments can be distinguished. The first one is payments. Payments are only indirectly involved in transforming savings into investments; their purpose is to transfer wealth. Transfers of financial wealth are essentially about managing information and hence are well served by digital technology. Arguably the most central of all financial compartments is that of intermediation. Intermediation directly connects savings and investments, the quintessential function of finance. Intermediation is essential for the economy, indeed for society as a whole, to prosper and grow. It can take place directly in the financial markets or through intermediaries: banks, insurance companies, pension and mutual funds, etc. In all cases, digitalisation is an essential component of the process. The remaining two compartments and their respective functions are diversification/hedging and arbitrage/spec-

[4] See FDIC (2023).

ulation. These functions support intermediation by making the management of financial assets and liabilities more efficient and (if properly handled) safer. The more advanced the economic system, implying more separation between savings and investment, the more the functions of diversification, hedging, arbitrage and speculation become important. All the above activities imply risks in different ways and to different extents. Payments are normally subject to lower risk relative to the other compartments because they deal with liquid instruments and are not involved in maturity transformation. By way of extreme synthesis, it is not incorrect to say that the first and the last two functions are ancillary to the second.

This framework can be used to discuss some of the most important manifestations of today's digital finance: cryptocurrencies, stablecoins, crypto-platforms, online payment platforms and smartphone applications, and central bank digital currencies (CBDCs). For each, we are interested in their potential contribution to a more 'complete' (meaning diversified, effective, efficient) financial sector, in their possible risks and the way to deal with them.

2. Cryptocurrencies

The best-known, most popular yet controversial 'actor' in today's digital finance universe is undoubtedly cryptocurrencies. According to a 2022 Pew Survey, nearly nine out of ten US citizens have at least some knowledge of them.[5] Bitcoin is by far the most popular cryptocurrency, dwarfing all others in its market capitalisation. At the peak of its popularity and price, around 2021, the market value of Bitcoin assets was comparable in size to the 6 largest US banks.[6]

Cryptocurrencies are 'outside assets', meaning that they aren't anybody's liability. Therefore, they do not (and cannot) play a role in the intermediation process but only serve potentially as means of payment or instruments for diversification, hedging or speculation.[7] Unlike other outside assets like gold or real estate, however, cryptocurrencies have no intrinsic user value. They derive their value – or maybe better, their price – from the interplay of demand and

[5] See Pew Market Research (2022).

[6] At the end of 2021 Bitcoin's market cap was roughly 1.3 tn US$, comparable in size to the 6 largest banks by assets – see S&P Global Market Intelligence (2021).

[7] Intermediation inherently requires inside assets, because the asset of the saver becomes the liability of the investor.

supply, both of which depend on the specific mechanisms that govern their creation.

Bitcoins are created through a process called 'mining,' the same used for the validation of transactions. Mining requires the solution of algorithms by computers on a competitive basis. The solution is complex, requiring huge amounts of computer power and energy to run these computers.[8] Mining is therefore very expensive and is rewarded by the attribution of new Bitcoins. If Bitcoins are pricey, as they have been especially in some periods, mining is worth it. Nobody knows exactly who or where these miners are. For sure they are not youngsters sitting in dormitory rooms in front of a laptop. Rather, they are immense computer installations placed in convenient locations – cost, tax and regulation-wise.[9]

According to internal rules, the total amount of Bitcoin that can ever exist is capped at 21 million. As we write, 19,427,769 bitcoins exist. This is probably one reason why many investors consider it valuable. If the maximum supply is fixed and demand matches it or even grows, the price will grow. Expectations of price rises prop up demand. This is a circular argument, but a powerful one. It explains why Bitcoin, and crypto in general, is sometimes likened to a 'Ponzi scheme,' although the trick invented by the Italian Carlo Ponzi in the early 1900s works differently.[10] It also explains why the Bitcoin price is very volatile. At very low levels from 2009 until 2017, the price rose above 56,000 euros per unit in 2020, before collapsing below 16,000 a year later. As we write, Bitcoin is staging a comeback at around 44,000 euros.

A different matter altogether is whether Bitcoin may, or may not, exercise the function of money or of a valuable portfolio asset. Hence the place it may or may not occupy as part of an efficient and diversified financial sector.

Validation of transactions is a slow process. It may take several minutes for each transfer of Bitcoins from one investor to another to be executed. The underlying distributed ledger technology (DLT) requires all participants to be

[8] See for example Dance (2023).

[9] A photo published by the Financial Times of a mining farm in Romania gives an idea, see here.

[10] Whether Bitcoin can be likened to a Ponzi scheme is debatable. In a Ponzi scheme, new investment inflows are used to remunerate or reimburse existing asset holders. This is not the case with Bitcoin. Since it lacks intrinsic value and capital gains are a major driver of new investor demand, the term 'bubble-cum-fraud' is probably appropriate. Ponzi-type constructs are not very far away, though. The US Security and Exchange Commission (undated document) found that virtual currencies such as Bitcoin can be used to enact Ponzi-type arrangements. Sam Bankman-Fried, the founder and former CEO of the collapsed crypto-exchange FTX, stated "… well, I'm in the Ponzi business and it's pretty good." See Alloway and Wiesenthal (2022).

informed of each transaction and potentially contribute to it. Philosophically, the DLT derives its attraction from the fact that it does not depend on any central authority responsible for the ledger. The underlying 'ideal' is to create a completely new asset, purely digital, independent of central authority or rule, outside established financial channels, and therefore – presumably – reliable and stable in value. A notion that echoes the 'free banking' concept popularised in the 19th and 20th centuries by theorists like F. Hayek and others.

Bitcoins, and cryptocurrencies in general, have so far failed in most of these objectives. They are not stable in value, as was noted before. Their transaction cost is huge, as are the energy consumption and environmental damage that mining entails.[11] They eschew traditional authorities and intermediaries like central or commercial banks but rely on an obscure oligarchy of miners outside of all democratic and regulatory control. For these reasons, it seems unlikely that they may in the foreseeable future perform at least part of the function of traditional established monies and monetary infrastructure and institutions – unless, of course, the latter end up being badly mismanaged.

However, even the harshest critics must recognise that Bitcoin and its peers have been remarkably resilient under adverse circumstances and shocks. High-profile failures and scandals have only dented their popularity temporarily. Regulatory initiatives, still in progress but fairly advanced in some jurisdictions, do not seem to discourage investors much. Many investors are prepared to hold cryptocurrencies in spite of the inherent risks. One reason may be their diversification value. According to the aforementioned Pew Survey, three out of four US investors in Bitcoin cite 'diversification' as their main motive (in addition to 'making money').

One cannot dismiss the possibility that cryptocurrencies may one day escape the fringes and become an established component of a more complete financial structure. However, this can only happen under certain conditions. First, the transparency and accountability of the creation and transaction processes need to be radically improved. This will require clear and extensive disclosure requirements, established and monitored by regulators. Limits must be established and enforced to protect small and unsophisticated investors. Crypto instruments are not for those who cannot evaluate and bear risk. Firewalls must exist between crypto markets and certain compartments of the traditional financial sector, like commercial banks, to prevent systemic risk. All these elements must apply on a global basis because of the inherent cross-border mobility of crypto.

[11] See Schmidt (2022).

The regulatory process is still in its infancy. The European Union has adopted legislative packages dealing with both market integrity and digital resilience, which are commented on elsewhere in this e-book. Regulators in the United States are not as advanced, having limited themselves so far to rules regarding the issuance of new crypto instruments and the AML dimension. We are still very far from global consistency.

3. Stablecoins

Stablecoins are classified as crypto-instruments because they normally use DLT, but have certain characteristics that set them apart from cryptocurrencies and bring them closer to traditional finance. Importantly, stablecoins – at least, the 'collateralised' category, which we will describe in a moment – are 'inside' assets. Hence, they play a role in the intermediation process.

Tether USD, or USDT, by far the largest stablecoin by capitalisation,[12] is 'collateralised' in the sense that it is structured as a traditional intermediary with a pool of purportedly safe assets backing the 'stablecoins' issued on its liability side.[13] What this pool exactly consists of, and how it is composed, is not fully clear, because stablecoins are not (yet) subject to the extensive disclosure requirements imposed on other intermediaries.[14] From the information available, they consist of bank deposits and short-term highly rated securities. These safe assets are supposed to guarantee that each unit of stablecoin tracks exactly the value of one US dollar.

The first representative of this asset class, the 'ancestor' of them all, was Libra, a failed attempt in 2019 by Facebook to launch a completely new and private global currency. According to the initial plan, Libra would have been collateralised by a multi-currency portfolio of safe assets. It should have become the money of choice of the wide and growing world population of Facebook users. Its designers, however, probably more versed in social media technology than in finance, underestimated the complications inherent in managing the risks of a multicurrency portfolio and the regulatory hurdles that this would entail. Eventually Libra was sold out and eventually abandoned. But the idea survived in different and less ambitious forms.

[12] See coinmarketcap.com (2023).

[13] See e.g. Hicks (2023).

[14] Information available on the reserves backing the Tether token, available in Tether (2023), is very limited.

Stablecoins occupy land between crypto and traditional finance. On the one hand, they are instruments of choice for cryptocurrency traders. On the other, the balance sheet structure of collateralised stablecoins closely mirrors that of money market funds (MMFs), where a pool of safe assets is supposed to preserve the monetary value of the liability they issue. The high-profile crises that money market funds have undergone in the last 50 years suggest that even the supposedly safest asset portfolio may not be sufficient to guarantee in all circumstances the 'moneyness' of the liabilities they are supposed to back up.[15]

However, considering that money market funds were a remarkable success story in the last half-century, one cannot rule out that stablecoins may also have a bright future. Again, however, there are conditions. On the one hand, the close complementarity with cryptocurrency markets suggests that the destinies of the two instruments are linked. The success or failure of one will depend on that of the other. On the other hand, collateralised stablecoins have an additional risk dimension: that of maturity transformation and diversification. Proper management can maintain risk at a minimum, but never eliminate it. Just as MMFs 'broke the buck' during the financial crisis, so can collateralised stablecoins. Regulation and supervision will be essential. The experience of MMFs suggests that regulating asset classes of a hybrid nature, at the intersection of money and securities markets, is not easy. Drawing boundaries is difficult and regulators may face considerable opposition from the industry.[16]

4. Crypto exchanges

Exchanges are infrastructure in which financial assets are negotiated, traded and settled. Hence, they mainly serve the last two functions of the four that we listed earlier. Securities payments also take place in them. Crypto exchanges are – like all exchanges – theoretically free from the risks of the underlying assets exchanged in them. In practice this is never the case, or at least not fully so. Client business is frequently combined with and to some extent requires a proprietary exposure. The risk involved depends on business models and is supposedly kept under control by effective regulation and supervision.

[15] See Bouveret, Martin and McCabe (2022).

[16] A wholly different asset class is that of algorithmic stablecoins, the value of which is not backed by collateral but supposedly guaranteed by a trading rule. This asset class, far less important than Tether and other collateralised instruments, came to prominence in May 2022 due to the failure of the s.c. Terra-Luna.

FTX, the largest and up to a certain point in time reputedly the most successful crypto exchange, established in 2019 and located in the Bahamas, spectacularly collapsed in a matter of a few hours in November 2021 and is now the object of numerous criminal court cases. FTX was an extreme manifestation of what can happen when combining a risky asset (crypto), a rogue business culture and practices, and inexistent regulatory oversight. The history is well-known[17] and needs not be repeated here.

FTX has disappeared but other large crypto exchanges continue to operate in remote locations essentially out of reach of global financial regulators. Their existence under a faulty regulatory umbrella implies constant risks for the global financial system. The experience of FTX has triggered a more proactive stance by global regulators, first by the US Securities and Exchange Commission. Efforts are being stepped up as we write[18] as regards crypto exchanges and crypto markets in general. It is unlikely that crypto assets can become a reliable component of the global financial landscape unless sound and transparent business models are enforced on crypto exchanges too.

5. Payment platforms and applications

Here we are squarely in the area of payments. Payment instruments and payment platforms are not exposed to position risk like other instruments that we have just discussed, but they are exposed to other and more subtle types of risks.

Digital payments have undergone a real ‘revolution’ in recent years, with a decisive contribution by technology firms. The use of paper (banknotes, personal cheques) in the payment system was gradually reduced, partly replaced initially by payment cards and then increasingly by online platforms and smartphone apps. There is no doubt that these changes have greatly improved the effectiveness and efficiency of the way people pay. The improvements have been significant in both advanced and developing countries. Digital payment technologies have also helped financial inclusion, particularly by facilitating access to advanced payment instruments in remote less-developed areas where banks are scarce, with positive effects on economic development.[19]

[17] A useful chronology can be found in Reuters (2022).

[18] A summary of recent initiatives is provided in Duggan (2023).

[19] See Beck et al. (2018).

These massive changes have not so far given rise to any significant risks or failures, technological or otherwise. Even during financial crises, the payment system as such has continued to work well. This is remarkable, considering that many completely new technologies have been introduced in a short period of time. In most countries, starting with the United States and the euro area, central banks play a central role in the oversight of payment systems in close co-operation with the legislative and executive branches. Crucially, all 'last generation' digital payment means, from credit to debit cards, from online platforms to smartphone apps, settle on bank accounts and eventually on central bank accounts. The support of the 'traditional sector' below the surface is invisible to retail users but it is essential to ensure the finality of payments and the stability of the overall system.

In the eurozone particularly, the interplay between public intervention and market forces in the area of payments has worked well. Regulatory action has not impeded rapid innovation and technological improvement engineered by both large technology firms and smaller fintech companies, increasingly in co-operation with the banking sector.[20]

6. Central Bank Digital Currencies (CBDCs)

In the last three or four years, central banks in most of the world have been exploring the possibility of introducing their own digital currencies, essentially digital forms of cash. Several factors have spurred this development. First, the increasing use of electronic payments has reduced recourse to paper currency in retail transactions (although cash is far from disappearing; demand for it has lately increased in most countries).[21] The rise of crypto markets was another element encouraging central banks to step in. Some central bankers have taken the view that the introduction of digital cash is necessary to keep central banks up to date in the digital era, even to ensure a solid 'anchoring' to mainstream currencies.

All these issues are actively debated in official and academic circles. Opinions differ on the impact CBDCs may have in various areas, from monetary policy

[20] By contrast, the US retail payment ecosystem remains fragmented, with competing payment applications not integrated with one another and a significant residual use of personal cheques. For one experience on the user side, see Angeloni (2023c).

[21] See for example Angeloni (2023b).

to financial stability, from the structure of payment systems to financial inclusion, from technological innovation to broader societal concerns like privacy and individual freedom.[22]
Few central banks have decided to introduce CBDCs so far, the main one being the People's Bank of China. Where they have been introduced, they have met mixed success, mainly because competition from private payment providers is strong and their added value unclear. Central banks in the Western world are researching and preparing, but no decision regarding the actual launch has been taken yet.

7. Concluding note

Digital finance is not new but it has been living a second youth since the turn of the century. New digital assets and new digital technologies to serve existing assets have appeared. In the area of retail payments, new technologies have become dominant, benefiting from a fruitful interplay of regulation and market forces. By contrast, in the area of cryptocurrencies and related instruments, regulation is still undeveloped, and experience has shown that investor risks are significant.

The future of finance is increasingly digital. Whether progress will be harmonious and socially beneficial will depend on how fast regulation picks up speed and proper safety, soundness, transparency and ethics standards are applied widely at a global level. Digital technology is borderless. Financial regulation cannot afford to be any less.

[22] The ECB has published three 'progress reports' on the subject and other material. See ECB (2023) and the links therein. This author's ideas are summarised in Angeloni (2023a).

References

Alloway T. and Wiesenthal J. (2022). *Sam Bankman-Fried Described Yield Farming and Left Matt Levine Stunned*. Bloomberg News, 22 April 2022.

Angeloni I. (2023a). *Digital euro: when in doubt, abstain (but be prepared).* April 2023, paper prepared for the Committee of Economic and Monetary Affairs of the European Parliament. Available here.

Angeloni I. (2023b). *The digital euro: what we know and what we don't.* OMFIF, 16 May 2023. Available here.

Angeloni I. (2023c). *Banking in US would make anyone a CBDC convert*. Financial Times, 17 September 2023. Available here.

Beck T., Pamuk H., Ramrattan R. and Uras B.R. (2018). *Payment instruments, finance, and development*. Journal of Development Economics, Volume 133, July 2018, Pages 162-186.

Bouveret A., Martin A. and McCabe P.E. (2022). *Money Market Fund Vulnerabilities: A Global Perspective*. Finance and Economics Discussion Paper, Federal Reserve Board, 12-2022.

coinmarketcap.com (2023). *Top Stablecoin Tokens by Market Capitalization*. Available here.

Dance G.J.X. (2023). *The Real-World Costs of the Digital Race for Bitcoin*. The New York Times, 9 April 2023.

Duggan W. (2023). *How does the SEC regulate crypto?*. Forbes, 30 June 2023.

ECB (2023) European Central Bank. *Digital Euro*. Available here.

FDIC (2023) Federal Deposit Insurance Corporation. *Crisis and Response, an FDIC History 2008-2013*. Chapter 1. Available here.

Fischer A. and McKenney J. (1993). *The development of the ERMA banking system; lessons from history*. IEEE Annals of the History of Computing. Vol. 15, No. 1, 1993.

Garbade K. and Silber W. (1979). *The payment system and domestic exchange rates; technological vs institutional change*. The Journal of Monetary Economics 5, 1979.

Hicks C. (2023). *What is Tether? How does it work?*. Forbes, 15 August 2023, Available here.

Pew Market Research (2022). *46% of Americans who have invested in cryptocurrencies say it's done worse than expected*. Available here.

Reuters (2022). *Rise and fall of crypto exchange FTX*. November 2022. Available here.

Tether (2023). Webpage *Transparency*. Available here.

Schmidt J. (2022). *Why does Bitcoin use so much energy?*. Forbes, 18 May 2022.

Securities and Exchange Commission (undated). *Ponzi schemes using virtual currencies*. Available here.

S&P Global Market Intelligence (2021). *The world's 100 largest banks*. Available here.

Section 2

Technologies and Drivers

1. Blockchain and DeFi – An economist's perspective for supervisors

Thorsten Koeppl

Professor of Economics, Robert McIntosh Fellow, RBC Fellow at the Department of Economics - Queen's University, and Part-time Professor of the Florence School of Banking and Finance at Robert Schuman Centre - European University Institute

1. Blockchain technology in financial markets

Over the last decade or so, 'blockchain' in financial markets has been associated with a fundamental transformation of the financial system in which intermediaries are replaced in favour of direct interactions among financial markets participants. More narrowly defined, blockchain refers to a particular form of distributed ledger technology (DLT) that allows anyone to directly participate in a distributed ledger. Such a ledger is "an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism."[1]

[1] See Regulation (EU) 2022/858. Blockchain as a technological term in computer science refers to a particular way of ordering information in a chronological sequence.

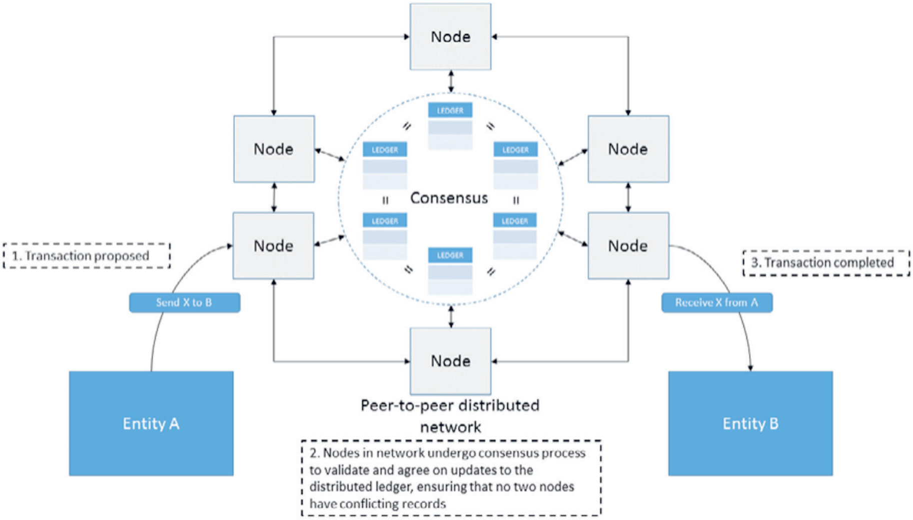

Node
Node
Node
LEDGER
LEDGER
LEDGER
Consensus
LEDGER
LEDGER
LEDGER
Node
Node
1. Transaction proposed
Send X to B
3. Transaction completed
Receive X from A
Node
Entity A
Peer-to-peer distributed network
Entity B
2. Nodes in network undergo consensus process to validate and agree on updates to the distributed ledger, ensuring that no two nodes have conflicting records

Figure 1: Schematic representation of a distributed ledger

Source: BIS (2017)

The technology originates from distributed computing and was popularised by Bitcoin, the first cryptocurrency. It relies on a digital representation of value and uses cryptography to secure and control ownership. The blockchain itself records ownership changes and is updated according to certain rules that are summarised in a consensus mechanism. Since 2017, with the rise of the Ethereum Blockchain, decentralised finance (DeFi) has expanded the use of the technology beyond cryptocurrencies to financial services such as trading, lending and asset management. Recently, a new ecosystem has emerged that offers an alternative to the traditional financial system which is largely based on the use of intermediaries such as broker-dealers, banks and asset management companies.

The value proposition of DeFi is much debated in the literature and among practitioners.[2] A common ledger among participants may help reduce back-office costs in financial markets and improve reconciliation of financial data. Its decentralised and more transparent nature may promise a more stable financial system. Reducing the influence of intermediaries is often seen as a precondition for a more open financial system leading to increased competition. Direct participation in financial markets may reduce the potential for fraud and for extracting rents from consumers. Before assessing these promises against current

[2] See Chiu et al. (2023) for a first attempt at measuring the value added of the DeFi ecosystem.

trends, it is useful to review the fundamental difference between the old and new financial systems.

2. Traditional finance vs. DeFi: It's all about trust

Traditional financial markets have evolved around trusted third parties that act as gatekeepers of the financial system by operating critical infrastructure such as payment, clearing and settlement, and by providing participants with financial services. In this role, they perform three core functions: custody, record-keeping and enforcement. First, as custodians they keep assets safe. Second, they maintain ownership records and update them when assets are transferred between owners. Finally, they ensure that financial contracts are executed and obligations in them are met.

The reason that intermediaries can take on these functions is that participants in financial markets trust them. Trust arises from the intertemporal incentives that intermediaries face. They charge fees for their services which creates a charter value through a future stream of income. Hence, it is costly for intermediaries to lose their reputation and risk their future income for short term gains at the cost of their customers.[3] Consequently, intermediation is necessarily costly in order to generate trust through intertemporal incentives, but it is often complemented with regulation that aims at maintaining trust in intermediaries.

Blockchain is often described as a 'trustless' system, or a system without a trusted third party running it. It relies on self-custody, in which the participants are in charge of safe-keeping their assets. In Bitcoin, for example, users have to store their bitcoins in wallets and are responsible for keeping their wallets safe. The system relies on distributed record keeping through a public blockchain that records either all transactions or maintains a list of all current owners of the assets. Finally, it relies on a consensus protocol that ensures that all participants agree on how to update records on the blockchain.

DeFi uses this approach to disintermediate financial services on the basis of 'decentralised trust.' This trust, however, is not costless to achieve. There are costs for individual participants to safeguard their assets. There are costs in developing applications and running the blockchain to keep records. And there

[3] Interestingly, the cost of intermediation has remained fairly constant at about 1.5-2% of intermediated assets [see for example Philippon (2015)]. One interpretation of this fact is that these costs are driven less by technology than by costs of providing proper incentives.

are costs in enacting changes to the blockchain associated with the consensus protocol.[4]

The best example is the cryptocurrency Bitcoin. It leverages ideas from computer science to employ a 'proof-of-work' protocol to record transactions and thus to update ownership of bitcoins. The protocol relies on energy-expensive computations in which so-called 'miners' compete to update the blockchain for a reward. This competition is designed to protect the blockchain against attacks in which malicious actors try to disrupt the blockchain or rational actors try to alter the blockchain in their favour.[5]

Intermediate solutions are also possible in which not a single intermediary but a specific group of participants provide some infrastructure or a service, which is often described as a 'permissioned blockchain.' Examples of such 're-intermediation' are a group of intermediaries such as banks replacing other intermediaries like infrastructure providers in payments or in securities. Trust is achieved within the group to the extent that the members of the group have mutual interests and that there are benefits from being part of the group.

A financial system built on decentralisation rather than intermediaries is therefore not automatically less costly or more efficient. It is helpful to think of the trade-offs involved in terms of the 'blockchain trilemma,' which is represented schematically in the figure below.

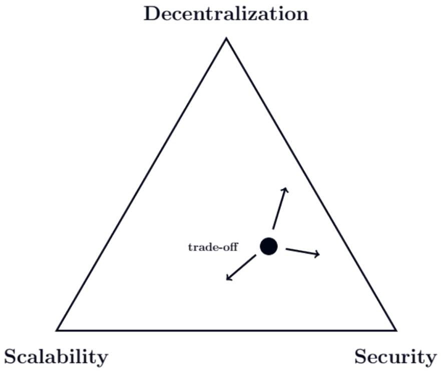


Figure 2: The Blockchain Triangle
Source: the author

[4] For a basic economic analysis of blockchain for cryptocurrencies and financial market infrastructure, see Chiu and Koeppl (2019).

[5] For a detailed analysis, see Chiu and Koeppl (2022).

The triangle represents the trade-offs involved in using decentralised systems from an economics perspective. Different designs of a system are represented by a circle inside or on the boundaries of the triangle. Consequently, any system can achieve at most two of three features perfectly, but never all three at the same time. Decentralisation refers to the degree of intermediation in the system. Scalability means the degree to which the system can sustain activity on the blockchain. Security expresses the degree of safety for users.

The bottom line is that there is not one optimal design for the financial system. Which point in the triangle will be chosen depends on the relative costs associated with the three apices of the triangle. It may vary with the particular application or with the participants in the financial system. Bitcoin and the traditional financial system occupy extreme positions on different faces of the triangle. Bitcoin is fully decentralised and given the design of its consensus protocol it is very secure. However, it faces tight restrictions on scalability. The traditional financial system is very scalable and secure but has a very low degree of decentralisation as it heavily relies on intermediaries. In addition, different consensus protocols put blockchain projects in different areas of the triangle.

In conclusion, it is hard to assess what structure is best for the financial system and different solutions may coexist reflecting different preferences of financial market participants. It is therefore likely that supervisors will have to face the reality of a mixed system in which decentralised solutions exist besides traditional intermediaries.

3. Current trends and challenges for supervisors

There are three broad developments that stand out for supervisors in financial markets. First, the degree of decentralisation in blockchain applications has been fairly limited. Most users do not directly participate in the technology at a fundamental level. Instead, new intermediaries – commonly labelled centralised finance (CeFi) – have entered the market to provide access to and services for the new DeFi ecosystem. Importantly, most problems in the blockchain and DeFi ecosystems so far have occurred at this level, with several blockchain projects, centralised crypto exchanges and stablecoin arrangements failing. Interestingly, all these failures were due to fundamentally unsound design or outright fraud. Similarly, only very few people participate directly in running the infrastructure and its applications. This has led to a significant degree of concentration. Examples are the dominance of large mining pools in Bitcoin and liquid staking pools in Ethereum, both at the heart of the consensus mechanism that substitutes for trust in a third party. Paradoxically, there is therefore a strong trend towards re-intermediation in blockchain and DeFi.

Second, the financial system has seen few fundamental changes arising from blockchain technology. Promising projects tend to fall in areas where there are naturally large frictions in financial transactions. For example, cross-border trading and payments (including remittances) may greatly benefit from distributed ledgers as this space sees much less trust than domestic financial markets and tends to be encumbered by difficult back office operations.[6] In line with financial technology (fintech), emerging economies may also benefit more from the technology, as there are often not relatively efficient legacy systems already in place. More generally, if there are large efficiency gains, one would expect that traditional intermediaries would start to harness the technology. Hence, in certain pockets of the financial system, the new technology may promise large efficiency gains with traditional intermediaries possibly being well positioned to achieve them.

Third, one area where blockchain potentially shows much promise is data and privacy. Intermediaries naturally sit at the interaction of information flows. The data generated by these flows have increasing financial value, and in many instances customers are not in control of how these data are being used. Blockchain provides at least pseudo-anonymity for its users. Currently, much research is taking place on providing Digital Identity Services in a blockchain environment. With the rise of data-driven finance, this technology may offer consumers a chance to regain control over their data so that they can monetise them in the marketplace.

Given these trends, what are then the main challenges supervisors face? Blockchain is a new technology but in the context of supervision many familiar themes arise for which existing knowledge can be used to provide guidance.

3.1 Consumer fraud

A key issue for blockchain is self-custody. Consequently, users are naturally exposed to custody risk and are likely to be unfamiliar with the technology. As has been pointed out, these features have given rise to new forms of intermediation, which create potential for consumer fraud.

[6] Blockchain technology has been a great vehicle to overcome policy-imposed frictions in financial markets. Examples are the use of crypto to circumvent capital controls and the use of cryptocurrencies as payment instruments in countries with higher inflation.

3.2 Regulatory arbitrage

Many applications duplicate existing financial services, but without regulatory compliance and a lack of proper risk control. Hence, it is crucial for supervisors to understand the value proposition of particular applications to weed out efforts that try to circumvent existing regulation in order to lower costs. Similarly, the regulatory framework needs to be adjusted to close the possibilities for such arbitrage.

3.3 Prominence of banking arrangements

The core of many arrangements in DeFi duplicates aspects of banking. One example are stablecoins, which either operate as a narrow bank, resemble fractional reserve banking or simply unbacked deposits. Other examples are collateralised lending and asset management. Hence, supervisors can follow guidance from banking regulation combined with applying new regulations such as MiCA.

3.4 High leverage and interconnectedness

DeFi often operates with extreme leverage and shows a high level of interconnectedness between different applications. A prominent example are decentralised lending arrangements, which are used to provide liquidity to a decentralised exchange. These risk factors are well understood by supervisors and they have the experience to assess them using the 'same risk, same rules' credo.

Looking at these themes gives one some comfort that supervisors will not be drowning or overwhelmed but will have a good handle on situations as they arise. Nevertheless, there are also some particular new unique challenges that come with blockchain technology and its applications.

First, while regulators and supervisors always tend to play catch up, innovation in blockchain and DeFi progresses at an immense pace. Hence, it will be difficult for authorities to keep up with new developments. Consequently, proactive regulation and supervision are necessary. However, supervisors also need to be mindful to not stifle innovation.

Second, regulatory and supervisory entry is difficult. It is often not clear who to actually regulate and supervise. With the emergence of CeFi, this problem has been somewhat alleviated. However, it becomes more acute the higher the degree of decentralisation is and therefore the more fundamental the blockchain application is. Is it the developer, the user or the governance token owner of the application that is responsible for regulatory compliance? Compounding the problem is the fact that many applications are designed to have users in different jurisdictions, requiring much international coordination and cooperation among supervisors.

Third, new intermediaries will compete with traditional financial intermediaries to apply blockchain technology in the best possible way. A prominent example are so-called Layer 2 Solutions offered by start-ups that build applications which only periodically rely on blockchains for their operation, but internalise many of the transactions on their own platform as traditional intermediaries do. Another example are BigTech companies that use blockchain technology to venture into payments, crypto assets and financial services.[7] It is not clear what the endgame will look like and what shape the financial system of the 21st century will ultimately take. Nevertheless, employing the principle of activity-based over entity-based regulation can help supervisors be a driving force in this transformation.

[7] The best example is the Libra/Diem project, which involved Facebook at the time and traditional intermediaries such as big banks and credit card networks in setting up an international currency.

References

BIS (2017) Bank for International Settlements. *Distributed Ledger Technology in Payment, Clearing and Settlement – An Analytical Framework*. Committee on Payments and Market Infrastructures.

Chiu J. and Koeppl T. (2019). *Incentive Compatibility on the Blockchain*. In Social Design – Essays in Memory of Leonid Hurwicz. Trockel, Walter (ed.), Springer.

Chiu J. and Koeppl T. (2022). *The Economics of Crytpocurrency: Bitcoin and Beyond*. Canadian Journal of Economics, 55 (4): 1762-1798.

Chiu J., Koeppl T., Yu H. and Zhang S. (2023). *Understanding DeFi Through the Lens of a Production-Network Model*. Bank of Canada, Staff Working Paper 2023-42.

Philippon T. (2015). *Has the US Finance Industry Become Less Efficient? On the Theory and Measurement of Financial Intermediation*. American Economic Review, 105 (4): 1408-38.

Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU.

2. Safe AI & ML

Paolo Giudici
Professor of Statistics at the Department of Economics and Management - University of Pavia

1. Background

Modern data-driven artificial intelligence (AI) enabled by powerful machine learning (ML) is rapidly changing financial services, leading to widespread diffusion of financial technologies (fintechs). While financial technologies bring important advantages (increased financial inclusion, better transparency, lower transaction costs) they may also lead to new risks. For example, peer-to-peer lending may result in contagion risk arising from the interdependence between borrowers generated by the fintech platform;[1] robo-advisors may generate a systemic risk component that derives from the multiple correlations present in a large collection of assets;[2] and digital means of payment may increase cyber risks[3] and systemic risk.[4]

The current widespread use of AI motivates a need to develop advanced statistical methods that can measure its trustworthiness, in line with the Artificial Intelligence Act (AI Act) recently proposed by the European Commission.[5]

[1] Giudici, Hadji-Misheva and Spelta (2020).

[2] Giudici, Polinesi and Spelta (2021).

[3] Aldasoro et al. (2022).

[4] Giudici and Abu-Hashish (2019).

[5] See EC (2021) COM(2021) 206 final.

Indeed, machine learning models are boosting artificial intelligence applications in many domains such as finance, health care and manufacturing. This is mainly due to their advantage in terms of predictive accuracy with respect to 'classic' statistical learning models. However, although machine learning models can achieve high predictive performance they have an intrinsic non-transparent ('black-box') nature. This is a problem in regulated industries as authorities responsible for monitoring the risks arising from the application of AI may not validate them. [6]

Accuracy and explainability are not the only desirable characteristics of a machine learning model. The European Artificial Intelligence Act introduces further requirements in a risk-based approach to AI applications, and classifies them in four risk categories: unacceptable; high risk (acceptable, but subject to risk management); limited risk (acceptable, but subject to disclosure); and minimal risk (always acceptable). Several applications of AI in finance, and in particular those that involve estimation of the creditworthiness of individuals or of companies, can be considered high risk, and therefore they require an appropriate risk management model. To develop such a model, we need to express the requirements of the AI Act and of similar regulations in terms of statistical variables, which can be measured with appropriate statistical metrics.

A similar context arose when the Basel II capital framework was released:[7] the market, credit and operational risk were identified as key statistical variables to assess the capital adequacy of a financial institution, and later with the Basel III revision[8] it was the turn of systemic risk. Meanwhile, statistical metrics such as value at risk and expected shortfall,[9] and later CoVaR,[10] have been proposed by researchers and later combined by banks and regulators in an integrated measure aimed at monitoring financial risks and coverage of them by banks' internal capital.

In a similar vein, we have identified from the AI Act four main statistical variables to measure sustainability, accuracy, fairness and explainability, which require the development of appropriate statistical metrics, eventually leading to an integrated S.A.F.E. measure of trustworthiness for a specific AI application, similar to the integrated financial risk of a financial institution in the

[6] Bracke et al. (2019).

[7] BIS (2004).

[8] BIS (2011).

[9] Artzner et al. (2001).

[10] Adrian and Brunnermeier (2016).

Basel regulations. The development of these metrics allows establishing not only whether an AI application is trustworthy but also the level of trustworthiness over time to be monitored by an artificial intelligence risk management model.[11]

From a methodological viewpoint, the statistical metrics that we propose consist of a set of four integrated statistical measures of trustworthiness, all based on an extension of the Lorenz curve[12] from measurement of income concentration to measurement of the concentration of machine learning predictions. The four statistical metrics can be summarised with the acronym S.A.F.E., which derives from the four variables considered: sustainability, which refers to the resilience of AI outputs to anomalous extreme events and/or cyber attacks; accuracy, which refers to the predictive accuracy of the model outputs; fairness, which refers to the absence of biases towards population groups induced by the AI output; and explainability, which refers to the ability of the model output to be understood and overseen by humans, and particularly the consequences that it drives. While the former two requirements are more technical and 'internal' to the AI process, the latter two are more ethical and 'external' to the AI process, involving the stakeholders of an AI system.

The proposed metrics consist of 'agnostic' statistical tools able to post-process the predictive output of a machine learning model in a general way independently of the underlying data structure and statistical model. With this aim, we have extended our recent paper[13] which proposed employing Lorenz zonoids,[14] the multidimensional version of the Gini index,[15] to improve on Shapley values,[16] one of the methodologies most employed to achieve explainability of otherwise 'black-box' machine learning models. Research[17] shows that employing 'Shapley-Lorenz' values allows measures of the explainability of each predictor in a machine learning model to be obtained, which, unlike Shapley values, are normalised between 0 and 1 and are expressed as a percentage of the overall predictive accuracy, rather than as a distance from the mean of the predictions like the classic Shapley values proposed by Shapley adapted

[11] Giudici et al. (2023).

[12] Lorenz (1905).

[13] Giudici and Raffinetti (2021).

[14] Koshevoy and Mosler (1996).

[15] Gini (1921).

[16] Shapley (1953).

[17] Giudici and Raffinetti (2021).

to the machine learning context.[18]

Lorenz zonoids can be employed as a basis to develop agnostic tools able to measure not only explainability but also accuracy, sustainability and fairness in a unified way, leading to an integrated measure of the trustworthiness of any artificial intelligence application.

The Lorenz curve was introduced[19] to measure the contribution to the wealth and income of a nation by each individual, or by each group of individuals, to assess economic inequalities in a nation's population and to measure the distance from an 'ideal' income distribution. It intuitively seems to be an appropriate tool to measure the contribution of each individual data point (or group of points) to the predictions of a machine learning model, in order to assess inequalities in the predictive outcomes of AI applications, in terms of single data points (sustainability) or of groups of points (fairness), and to measure the distance of the predictions from the response to be predicted (accuracy). The same concept can furthermore be employed to measure the contribution to the predictions of each explanatory variable by each data point or group of points, allowing the Shapley-Lorenz measure proposed in our previous paper[20] to become a local measure of explainability.

Among high-risk applications of AI in finance, the European AI Act explicitly mentions assessment of the creditworthiness of individuals and companies, which is also known as credit scoring. Credit scoring is a predictive classification problem which has attracted many researchers, who have employed various statistical learning models to measure it. It is no surprise that modern machine learning methods have found in credit scoring one of their first fields of application in economics.

The recent credit scoring literature[21] reveals a general consensus on the superior predictive accuracy of machine learning models based on ensemble methods, such as random forest and gradient boosting, with respect to classic learning models, such as logistic regression, classification trees and bayesian networks. The increased accuracy comes, however, at a cost: while classic models are 'explainable' as they can clearly identify the contribution of each explanatory variable to the credit score, ensemble methods are 'black boxes' and cannot explain to their users the determinants of credit scores. Related to this,

[18] Lundberg and Lee (2017).

[19] Lorenz (1905).

[20] Giudici and Raffinetti (2021).

[21] Tripathi et al. (2022).

it is difficult to understand whether these models are fair and unbiased with respect to different population groups.

To overcome this problem, ensemble methods should be complemented with explainable AI methods that are to be applied *a posteriori* to the credit scores obtained. Among these, the most important are the Shapley values method[22] and the LIME method.[23] These explainable AI methods have recently been increasingly applied to credit scoring problems, starting in the works of Bussman et al.[24] and Moscato et al.[25] Their empirical results show the ability of explainable AI methods to achieve both predictive accuracy and explainability.

With the aim of achieving a general approach to measuring the trustworthiness of AI applications in finance, Lorenz zonoids can be leveraged to derive statistical metrics that extend those in previous works. Such metrics are able to assess not only accuracy and explainability but also sustainability and fairness in an integrated way with metrics that are themselves normalised and the significance of which can be evaluated by means of appropriate statistical tests. This will allow all credit market participants (borrowers, lenders, regulators) to assess the trustworthiness of AI for credit scoring using a common language.

2. Proposal

The S.A.F.E. model that we propose is made up of four components, which we now illustrate, particularly in terms of their policy implications. The first component focuses on accuracy, which is pivotal to the whole structure. A key point for policymakers required to assess the accuracy of a machine learning model, and more generally of any data-driven statistical learning model, is evaluation of its predictive accuracy. A predictive accuracy tool can evaluate and monitor over time the quality of predictions, and possibly replace the model with a better performing one. This is well known in the statistics literature. For a review, see, for example, Gneiting.[26]

The traditional paradigm in the literature compares statistical learning models in a model selection procedure in which a model is chosen through a sequence of pairwise comparisons of the likelihoods (or of the posterior probabilities) of the models being compared. These criteria are not generally applica-

[22] Lundberg and Lee (2017).

[23] Ribeiro et al. (2016).

[24] Bussman et al. (2021).

[25] Moscato et al. (2021).

[26] Gneiting (2011).

ble when the underlying probability model is not specified as in the majority of machine learning models, such as neural networks and ensemble tree models.

To overcome this problem, and in parallel with the increasing availability of computational power, which has boosted the application of machine learning models, the last few years have witnessed a growing importance of model comparison methods based on comparison between the predicted and the actually observed cases, typically in cross-validation methods. In cross-validation, the data are split in two or more datasets, with a 'training' dataset used to fit a model and 'validation' or 'test' datasets used to compare the predictions made by the fitted model with the actual observed values.

Examples of predictive problems are the classification of credit borrowers in rating classes in the credit lending context, and prediction of asset prices in asset management settings.

In the cross-validation setting, the response variable determines which predictive accuracy measure to use. Specifically, when the response variable is continuous, the most employed accuracy measure is root mean squared error (RMSE) based on the Euclidean distance of the predictions from the actual values, related to Pearson's correlation coefficient.

When the response variable is ordinal (as in the credit rating example) the Euclidean distance can still be applied, replacing the predicted and actual values with their ranks, leading to Spearman's correlation coefficient or to Kendall's tau. When the response variable is binary, the predictive accuracy can be evaluated with the Brier score, which, like Sperman's and Kendall's, employs a Euclidean distance. Alternatively, predictive accuracy can be measured in terms of the distance between predicted and actual probability forecasts of both 0 and 1 values, giving rise, when different cut-off thresholds are considered, to the receiver operating curve, and the area under it (AUROC) as the main summary measure.

All the previous accuracy measures depend on the type of response variable, and none of them can be universally applied, thus limiting the autonomy of AI applications. To solve this problem we propose a new measure that can be universally applied regardless of the nature of the underlying response variable. To this end, we suggest comparing the Lorenz zonoid of the response variable with the concordance curve obtained by ordering the response values in terms of the predicted values. It can be shown that in the binary case the area between the concordance curve and the dual Lorenz curve, properly normalised, is equivalent to the well-known area under the receiver operating characteristics (AUROC). However, the area under the concordance curve can also be calculated in the same fashion for ordinal and continuous variables, giving rise to very general accuracy metrics. A further advantage is its robustness, which derives from the nature of Lorenz zonoids, which can be related to the Gini measure based on the notion of mutual variability, which are more robust to outlier observations than the variability from the mean measured with the variance. [27]

The second component of the S.A.F.E. model we consider concerns measurement of the sustainability of a model. Sustainability, understood as the 'robustness' of model results under extreme changes due to a changing environment or to cyber attacks, can also be measured by means of Lorenz curves, like accuracy. This, in line with the nature of Lorenz curves, allows inequalities in point predictions to be identified, which may indicate that the model is not resilient to anomalous data.

From a policy viewpoint, the sustainability requirement means that the model results are stable under variations in the data, and in particular when extreme data resulting from stress scenarios and/or from cyber data manipulations are included in the training, validation or test data sets.

To improve the sustainability of AI applications, we also propose extending the variable selection methods available for probabilistic models to non-probabilistic models such as ensemble models and neural network models, using statistical tests based on a comparison of the Lorenz zonoids of the predictions. This extension provides a model selection criterion for machine learning models without a specified probabilistic model, a comparison that is not possible in the current state of the art.

The selection of a parsimonious (and therefore more sustainable) model can be obtained by building a sequence of pairwise comparisons of machine learning models, each of which is obtained from the previous one by adding (or deleting) one variable. For each comparison, statistical tests of the equality of Lorenz zonoids can be employed, extending the results in Schechtmann et al.[28] and providing a model comparison criterion that can be applied to any machine learning model, not only to those that satisfy specific assumptions, extending the De Long test[29] for binary variables and the Diebold and Mariano test[30] for continuous variables.

Lorenz zonoids can be employed not only to improve sustainability by means of model selection but also to measure how sustainable a given model

[27] Olkin and Yitzhaki (1992).

[28] Schechtmann et al. (2008).

[29] De Long et al. (1988).

[30] Diebold and Mariano (1995).

is with extreme data points or cyber data manipulation. This can be achieved by comparing the predictive accuracy of a model as measured by its Lorenz zonoid in different ordered subsets of the data, from the best to the worst fitting values, partitioning the data, for example, in deciles. We can then calculate the Gini concentration index of the Lorenz zonoid values. A high value of the index (close to one), indicating concentration, will mean that the model is not sustainable, being heavily affected by data variations. Conversely, a low value of the Gini index (close to zero), indicating equality, will mean that the model is sustainable.

The third component of the S.A.F.E. model aims to measure explainability. With this aim we employ Shapley-Lorenz values[31] to measure the contribution of each potential explanatory variable in percentage values of the overall predictive accuracy. This leads to a measure of explainability which extends Shapley values and LIME approaches. The advantage of the Shapley-Lorenz measure is that it expresses how much a variable explains (as a percentage) of the total variability. This is a normalised and easy to interpret measure, unlike Shapley and LIME values, the values of which are more difficult to interpret. From a policy viewpoint, explainability allows the variables which most impact the outputs of a machine learning model to be identified.

The fourth component of the S.A.F.E. model concerns measurement of fairness. Fairness is a property that requires that an AI application does not lead to biases among different population groups described by appropriately chosen control variables such as gender, race and nationality. The recent literature on algorithmic fairness has proposed different ways to measure fairness (see, e.g., Mitchell et al.[32] and Kozodoi et al.[33]). Some are conditional on the predictor variables employed and some are unconditional. In the SAFE-FAI project we aim to develop a general measure of fairness which can be applied both conditionally and unconditionally. To achieve this aim we will extend the Gini coefficient, which was originally developed to measure the concentration of income in a population, to measurement of the concentration of the predictions of a machine learning model in terms of their Shapley-Lorenz values. For a given set of selected explanatory variables, Shapley-Lorenz values which are similar among the groups lead to a Gini coefficient close to 0, indicating that the effect of these variables is fair across different population groups. On the

[31] Giudici and Raffinetti (2021).

[32] Mitchell et al. (2021).

[33] Kozodoi et al. (2022).

other hand, a Gini coefficient close to 1 indicates that the effect of the variables on the response largely depends on some groups, highlighting a bias, possibly due to data that are not equally representative. The Gini coefficient can be supplemented with a statistical test, thus extending the recent contribution by Agarwal et al.[34], who employ Shapley-Lorenz values[35] to test for racial discrimination in credit lending. From a practical viewpoint, they show that the (unconditional) Shapley-Lorenz importance of the race of the applicant is 10 times higher when using a logistic regression rather than a random forest model, indicating the superiority of ensemble models, not only in terms of accuracy but also fairness.

From a policy viewpoint, the four scores received for each model, in terms of predictive accuracy, explainability, sustainability and fairness, all normalised between zero and one, give rise to an overall score that can be used to monitor the risk of any AI application. Thanks to their common mathematical derivation, the four scores and the related statistical tests can be integrated in a single normalised measure that can be monitored over time.

Giudici and Raffinetti[36] is a longer version of what is presented here with an example of how the methodology can be applied to a real machine learning problem.

[34] Agarwal et al. (2023).

[35] Giudici and Raffinetti (2021).

[36] Giudici and Raffinetti (2023).

References

Adrian T. and Brunnermeier M. (2016). *CoVaR*. American Economic Review, 106 (7), 1705-1741.

Agarwal S., Muckley C. and Neelakantan P. (2023). *Countering racial discrimination in algorithmic lending: a case for model agnostic interpretation methods*. Economics letters, 226.

Aldasoro I., Gambacorta L., Giudici P. and Leach, T. (2022). *The drivers of cyber risk*. Journal of Financial Stability, 60, 100989.

Artzner P., Delbaen F., Eber J.M. and Heath D. (2001). *Coherent measures of risk*. Mathematical Finance, 9 (3), 203-228.

BIS (2004) Bank for International Settlements. *Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework*. Basel Committee on Banking Supervision, 10-6-2004.

BIS (2011) Bank for International Settlements. *Basel III: A global regulatory framework for more resilient banks and banking systems*. Basel Committee on Banking Supervision, 1-6-2011.

Bracke P., Datta A., Jung C. and Sen S. (2019). *Machine learning explainability in finance: an application to default risk analysis*. Bank of England Working Paper, 816.

Bussman N., Giudici P., Marinelli D. and Papenbrock J. (2021). *Explainable machine learning in credit risk management*. Computational economics, 2021, 57 (1), 203-216.

DeLong E.R., DeLong D.M. and Clarke-Pearson D.L. (1988). *Comparing the areas under two or more correlated receiver operating characteristic curves: a nonparametric approach*. Biometrics, 44(3), 837-845.

Diebold F. and Mariano R. (1995). *Comparing Predictive Accuracy*. Journal of Business and Economic Statistics, 13 (3), 253-263.

EC (2021) European Commission. *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.* COM(2021) 206 final.

Gini C. (1921). *Measurement of Inequality of Incomes*. Economic Journal, 31, 124-126.

Giudici P. and Abu-Hashish I. (2019). *What determines bitcoin exchange prices: a network VAR approach*. Finance Research Letters, 28, 309-318.

Giudici P., Hadji-Misheva B. and Spelta A. (2020). *Network based credit risk models*. Quality Engineering, 32(2), 199-211.

Giudici P., Polinesi G. and Spelta A. (2021). *Network models to improve robot advisory portfolios*. Annals of operations research, 313 (2), 965-989.

Giudici P. and Raffinetti E. (2021). *Shapley-Lorenz eXplainable Artificial Intelligence*. Expert systems with applications, 167, 114104.

Giudici P., Centurelli M. and Turchetti S. (2023). *Artificial Intelligence Risk Measurement*. Expert Systems with applications, 235, 121220.

Giudici P. and Raffinetti E. (2023). *SAFE Artificial Intelligence in Finance*. Finance Research Letters, 56, 104088.

Gneiting T. (2011). *Making and evaluating point forecasts*. Machine Learning, 45, 171-186.

Koshevoy G. and Mosler K. (1996). *The Lorenz Zonoid of a Multivariate Distribution*. Journal of the American Statistical Association, 91, 873-882.

Kozodoi N., Jacob J. and Lessmann S. (2022). *Fairness in credit scoring: assessment, implementation and profit implications*. European Journal of Operational Research, 297, 1083-1094.

Olkin I. and Yitzhaki S. (1992). *Gini regression analysis*. International Statistical Review, 60 (2), 185-196.

Lorenz M.O. (1905). *Methods of measuring the concentration of wealth*. Publications of the American Statistical Association, 9, 209-219.

Lundberg S.M. and Lee S. (2017). *A unified approach to interpreting model predictions*. Advances in Neural Information Processing Systems, (NIPS 2017), 30, 4768-4777.

Mitchell S., Potash E., Barocas S., D'Amour A. and Lum K. (2021). *Algorithmic fairness: choices, assumptions and definitions*. Annual review of statistics and its applications, 8, 141-163.

Moscato V., Picariello A. and Sperli G. (2021). *A benchmark of machine learning approaches for credit scoring predictions*. Expert systems with applications, 165 (1), 113986.

Passach D. and Shmueli E. (2022). *A review on fairness in machine learning*. ACM Computing Surveys, 55(3), 1-44.

Ribeiro M.T., Singh S. and Guestrin C. (2016). *Why Should I trust you? Explaining the predictions of any classifiers*. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135-1144.

Schechtman E., Yitzhaki S. and Artsev Y. (2008). *The similarity between mean-variance and mean Gini: Testing for equality of Gini correlations*. Advances in Investment analysis and portfolio management, 3, 97-122.

Shapley L.S. (1953). *A value for n-person games*. Contributions to the Theory of Games II. Princeton University Press, 307-317.

Tripathi D., Shukla A.K., Reddy B.R., Bopche G.S. and Chandramohan D. (2022). *Credit scoring models using ensemble learning and classification approaches: a comprehensive survey*. Wireless Personal Communications, 1-28.

3. Artificial intelligence and machine learning in the hearts of central banks and supervisors: A case study of the Dutch central bank[1]

Patty Duijm
Head of Department Securities, Sustainability and Payment Statistics at De Nederlandsche Bank

Iman van Lelyveld
Head of Department Data Science Hub at De Nederlandsche Bank, Professor of Financial Markets and Banking at VU Amsterdam, and Part-time Professor of the Florence School of Banking and Finance at Robert Schuman Centre - European University Institute

1. Introduction

New data sources and new techniques are rapidly providing new possibilities for supervisors to improve the tools they have at their disposal. Such tools are

[1] The content of this chapter reflects the opinions of the individual authors and does not necessarily reflect the views of De Nederlandsche Bank.

known as ‘SupTech’ and they allow supervision to become more efficient or have more comprehensive risk capture.

In this chapter we present a case study on how to effectively ingrain data science based on our experience at a central bank [De Nederlandsche Bank (DNB)], the Dutch Central Bank). These data science techniques are also commonly known as artificial intelligence (AI) or machine learning (ML)[2] Following a trial in the Statistics division, data science in the Dutch Central Bank was formalised by the establishment of the Data Science Hub (DSH) in 2020. The DSH is the hub in a hub-and-spoke model, working with the various divisions across both the central bank, supervision, and resolution. It is tasked with promoting data-driven ways of working and fostering the data science community.

The aim of the present chapter is straightforward. We demonstrate the huge potential of data science in seven lessons, all supported by our own projects. With these descriptions, we hope to inspire others.

2. DNB’s experiences

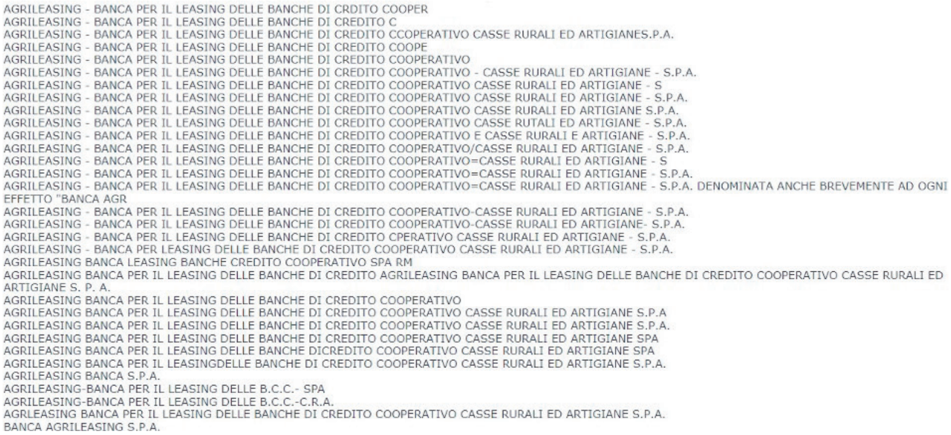
2.1 Granular data sets

The 2008-2010 crisis showed that authorities were missing crucial information to accurately identify risks in the financial system. This realisation led to a significant increase in the volume and granularity of data that financial institutions are required to report. For Europe, for example, granular information on credits (AnaCredit), money markets transactions (MMSR, SFTR), derivative trades (EMIR), security holdings (SHS) and trading (MiFID) is being collected. Although data quality issues remain, these data sets allow unprecedented coverage of all major activities in the financial sector at a very granular level.

[2] Following the definition of Nasution (2020), we define data science as the extraction of knowledge from high-volume data, using skills in computing science, statistics and specialist domain knowledge of experts. As for tooling, we almost exclusively use open source coding languages (mostly Python, some R). These languages are developing extremely fast and are designed to collaborate (also with other frameworks). Internally, code is, in principle, free to share through Azure DevOps (or ADO). DNB has decided to treat code as data and apply the existing sensitivity framework. Externally, the DSH operates the DNB Github that hosts our publicly available packages. Although for real development we use an integrated development environment (IDE, e.g. Visual Studio Code), Jupyter Notebooks are invaluable to let people interact and experiment with code and data. As for statistical methods, we take a pragmatic approach and try to solve the issue at hand with the simplest method possible rather than the most fancy one [see Chakraborty and Joseph (2017) for an excellent overview of relevant methods]. We are in close contact with teams that focus on Business Analytics (i.e. dashboarding in Power BI) or Robotic Process Automation (RPA).

Combining the new granular data in a coherent framework would allow an even better understanding of the dynamics of the European financial system. Here, some challenges remain. We list three of the main challenges we have encountered and show how we coped with them.

First, in many cases, reporting agents are free to submit counterparty names as free-form text. As Figure 1 shows, exposures to the same agent can therefore be labelled slightly – or completely – differently, underestimating the concentration of risks. To map a differently spelled counterparty to a single and unique identifier we have developed a 'fuzzy name matching' package, which is available on Github.[3]



```
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CRDITO COOPER
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO C
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO CCOPERATIVO CASSE RURALI ED ARTIGIANES.P.A.
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPE
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO - CASSE RURALI ED ARTIGIANE - S.P.A.
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO CASSE RURALI ED ARTIGIANE - S
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO CASSE RURALI ED ARTIGIANE - S.P.A.
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO CASSE RURALI ED ARTIGIANE S.P.A.
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO CASSE RUTALI ED ARTIGIANE - S.P.A.
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO E CASSE RURALI E ARTIGIANE - S.P.A.
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO/CASSE RURALI ED ARTIGIANE - S.P.A.
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO=CASSE RURALI ED ARTIGIANE - S
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO=CASSE RURALI ED ARTIGIANE - S.P.A.
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO=CASSE RURALI ED ARTIGIANE - S.P.A. DENOMINATA ANCHE BREVEMENTE AD OGNI
EFFETTO "BANCA AGR
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO-CASSE RURALI ED ARTIGIANE - S.P.A.
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO-CASSE RURALI ED ARTIGIANE- S.P.A.
AGRILEASING - BANCA PER IL LEASING DELLE BANCHE DI CREDITO CPERATIVO CASSE RURALI ED ARTIGIANE - S.P.A.
AGRILEASING - BANCA PER LEASING DELLE BANCHE DI CREDITO COOPERATIVO CASSE RURALI ED ARTIGIANE - S.P.A.
AGRILEASING BANCA LEASING BANCHE CREDITO COOPERATIVO SPA RM
AGRILEASING BANCA PER IL LEASING DELLE BANCHE DI CREDITO AGRILEASING BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO CASSE RURALI ED
ARTIGIANE S. P. A.
AGRILEASING BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO
AGRILEASING BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO CASSE RURALI ED ARTIGIANE S.P.A
AGRILEASING BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO CASSE RURALI ED ARTIGIANE S.P.A.
AGRILEASING BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO CASSE RURALI ED ARTIGIANE SPA
AGRILEASING BANCA PER IL LEASING DELLE BANCHE DICREDITO COOPERATIVO CASSE RURALI ED ARTIGIANE SPA
AGRILEASING BANCA PER IL LEASINGDELLE BANCHE DI CREDITO COOPERATIVO CASSE RURALI ED ARTIGIANE S.P.A.
AGRILEASING BANCA S.P.A.
AGRILEASING-BANCA PER IL LEASING DELLE B.C.C.- SPA
AGRILEASING-BANCA PER IL LEASING DELLE B.C.C.-C.R.A.
AGRLEASING BANCA PER IL LEASING DELLE BANCHE DI CREDITO COOPERATIVO CASSE RURALI ED ARTIGIANE S.P.A.
BANCA AGRILEASING S.P.A.
```

Figure 1: The case for Fuzzy Name Matching

This figure shows how one unique institution may show up in datasets with many differently spelled names, providing a clear case for our fuzzy name matching package.
Source: DNB DSH project documentation.

Second, an issue in merging granular datasets is that not all entities included in the data have a single unique identifier. After the global financial crisis, the Legal Entity Identifier (LEI) was introduced. The potential of the LEI for supervisors, financial markets and institutions is enormous. It not only introduces unique firm identifiers (so-called level 1 data) but also contains information on ownership structures (level 2 data). Thus, one is able to, for example, plot intra-firm networks as is shown in Figure 2. At the DSH, we have attempted to measure intra-firm complexity using LEI data, but we soon found that substantial data issues, among which is the current low coverage of the data, impede its use.[4]

[3] Nijhuis (2022).

[4] Rietveld, Lange and Duijm (2023).

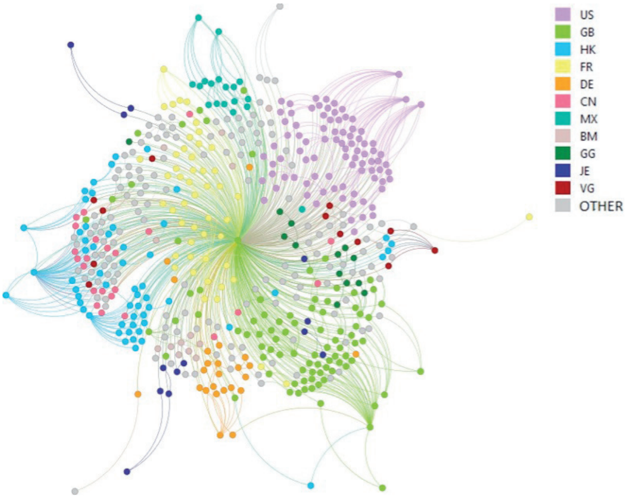


Figure 2: Intra-firm networks using LEI data

This figure plots the intra-firm network of HSBC Holdings PLC. Every dot represents an entity with a LEI code that belongs to HSBC Holdings PLC. The colours of the nodes represent the country of the reporting entity.

Source: Rietveld, Lange, and Duijm (2023).

Third, by focusing on one specific topic, one may simply not get the complete picture. For example, due to the over-the-counter (OTC) nature of derivatives markets there is no centralised overview of the market. Participants only observe their own volumes and exposure concentrations. The major US investment banks therefore did not realise that jointly they were massively exposed to a single entity, the lightly regulated insurer AIG. In setting their capital buffers and implementing other risk mitigating procedures, they were therefore ignoring an important yet unobserved concentration risk. In one of our projects we have combined several granular data sets with the aim of coming to a comprehensive view of exposures of Dutch banks on non-bank financial institutions (NBFIs).[5] The data included comes from AnaCredit, Securities Holdings Statistics (SHS), the Securities Financing Transactions Regulation (SFTR) and the European Market Infrastructure Regulation (EMIR). We have combined these data sets by using the aforementioned LEI information and data obtained from the Register of Institutions and Affiliates Database

[5] We are not the first to do this. See Hüser and Kok (2019). Furthermore, see the survey by Hüser (2015) for an overview of the multilayer financial network literature.

(RIAD). With this we have delivered a comprehensive view of exposures to the Dutch NBFI sector, as is shown in Figure 3. Given the confidentiality of some of these data sources we do not show the output here. We can, however, say that the established network clearly shows that Dutch banks are exposed to NBFIs via multiple linkages. Therefore, for concentration risk, one should not focus solely on a single source of exposure but take into account different sources.

2.2 Combining internal and external sources

The data a central bank receives through regular reporting can become even more informative if we add additional non-traditional data. For example, Van Dijk and De Winter extract topics from a large corpus of Dutch financial news (spanning January 1985 to January 2021) and investigate whether these topics are useful for monitoring the business cycle and nowcasting GDP growth in the Netherlands.[6] Their newspaper sentiment indicator has high concordance with the business cycle and increases the accuracy of DNB's nowcast of GDP growth, especially in periods of crisis. Therefore, tone-adjusted newspaper topics seem to contain valuable information not embodied in traditional monthly indicators from statistical offices.

Of course, adding other data is not a new idea. Hedge funds, for example, have been using 'alternative data' for decades. One of the first companies to use alternative data like satellite imagery, web scraping and other creatively sourced datasets was Renaissance, a hedge fund looking for an edge in trading. A big bank like UBS uses satellite imagery of big retailers' car parks and correlates car traffic with quarterly revenue, generating accurate predictions of earnings before they are released.[7]

[6] Van Dijk and De Winter (2023).

[7] The founder of Walmart, Sam Walton, would fly over parking lots in the 1950s in person to do pretty much the same thing.

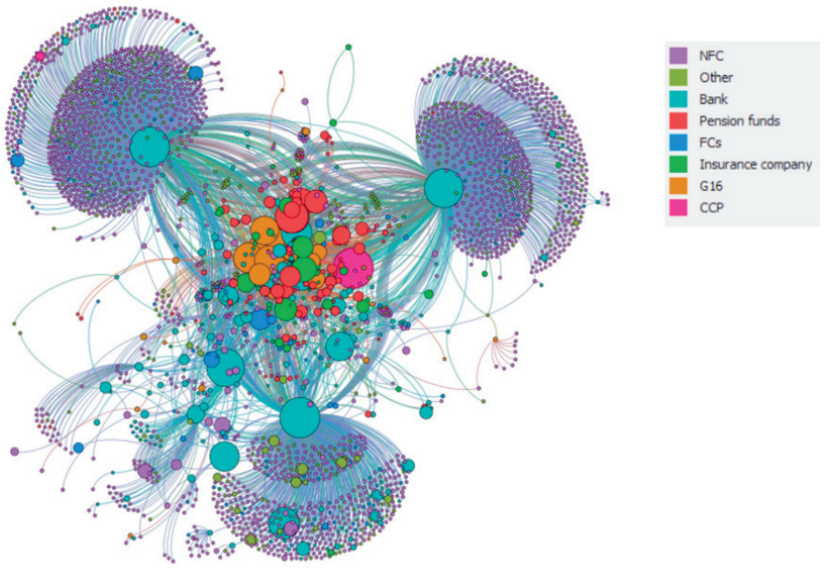


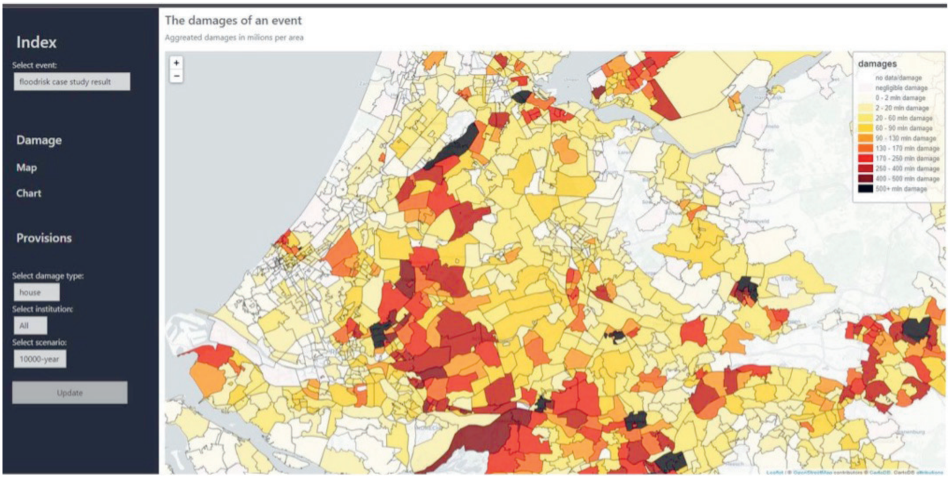
Figure 3: NBFI network using granular data

This figure shows how Dutch financial institutions are exposed to NBFIs through multiple sources.

Source: van den Boom, Hofman, Jansen and van Lelyveld (2021).

In cooperation with the BIS Innovation Network, the Data Science Hub has developed a digital twin pilot of climate risks. Here, a digital twin is defined as a digital representation of a real-world entity or system.[8] In this pilot, the digital twin was developed to measure the effects of climate events on the financial system via real estate exposures of financial institutions. For the Netherlands a flood risk case has been assessed. Insight into the spread of flood risk was obtained based on existing research on damage caused by specific water depths. Zipcode maps in combination with basic house information and housing price statistics were used to map real estate exposures to the flood map and determine estimated losses for the financial industry (i.e. banks and insurance companies).

[8] This definition is obtained from Gartner. See Jones et al. (2020) for a detailed explanation of Digital Twins.



The damages of an event

Aggreated damages in milions per area

Select event: floodrisk case study result

Select damage type: house

Select institution: All

Select scenario: 10000-year

Figure 4: A Digital Twin pilot for climate risk

This figure shows estimated damages to the Dutch financial industry in the case of a flood risk scenario (with an estimated probability of once in 10,000 years).

Source: DNB DSH project documentation.

2.3 Automating data processes

Until relatively recently, the typical workflow was that data was collected manually from either internal or external sources. Often wrangling the data was a labour-intensive job in Excel. Such manual processes are not only expensive but also prone to human error. For example, for DNB's internal inflation prediction model external data was collected from various sources on a regular basis as input for the model. In fact, multiple processes within the central bank use external data sources, resulting in colleagues collecting (the same) data manually or via ad hoc scripts. This may also result in cases in which different (or even outdated) versions of the same data set are used in DNB. The left-hand panel of Figure 5 displays this situation.

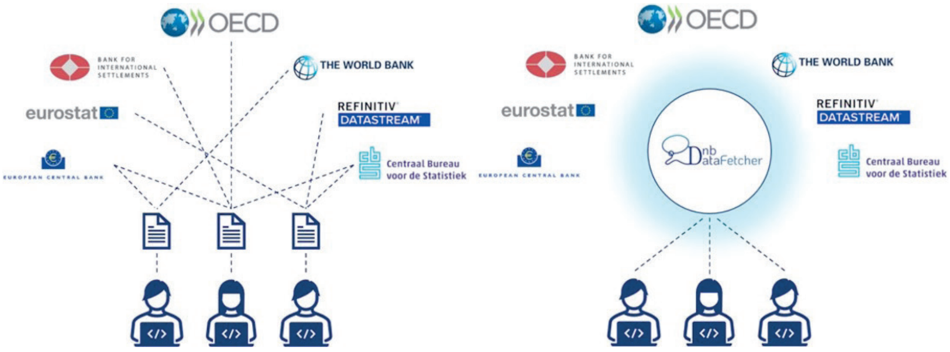


Figure 5: The DNB DataFetcher
Source: DNB DSH project documentation.

In an ideal situation, i.e. the right-hand panel of Figure 5, colleagues in the same institution have immediate access to the same data, while restrictions dictated by privacy and confidentiality should be respected. Therefore, as well as to open a discussion on how to modernise data workflows, we developed DataFetcher.[9]

The DataFetcher is a Python package that acts as a wrapper on top of publicly available application programming interfaces (APIs) granting access to various public data sets (e.g. IMF, OECD and ECB). Users no longer need to understand all the separate APIs but can download data using unified syntax. Working closely with users in development allowed us to establish trust and leave users in control. Once the DataFetcher was established, we started on infrastructure to collect the necessary data and fill a database on Azure – our cloud provider. Again, working closely with the modelling department allowed transfer of skills and establishing a sense of comfort with this new way of working. This approach is known as BizDevOps (developing and operating close to or by the users) and it is especially effective if requirements are fluid or to be fleshed out in the process.

The next step we are working on now is to be able to automatically run models in the cloud. The ultimate goal here is to be able to initiate a forecast from a smartphone. It is not our ambition to conquer the market with this app but the ability to quickly and painlessly change some part of the process allows for more flexibility in the development process. For example, it will be much easier to change the inflation forecasting model to incorporate unanticipated energy crises or pandemics. This, in turn, will improve policymakers' ability to timely react to unforeseen events in a timely manner.

[9] The package is available to ESCB NCBs.

2.4 Outlier detection

An important part of both the compilation of statistics and supervision is to identify observations that are out of the ordinary. That is, outlier detection. In this section, we cover two projects that focus on outliers: first, an approach in which we implement reinforcement learning in granular prudential reporting, and second, use case in the realm of Know Your Customer (KYC).

The first use case is one in which we implement a reinforcement learning algorithm.[10] Outliers are often present in data, and many algorithms exist to find them. Often we can verify outliers to determine whether or not they are data errors. Traditionally, outliers are identified using 'business rules' – ground truths that are valid by definition or result from experience. Assets should equal liabilities, for example. However, defining and hard-coding business rules is cumbersome. Also, in some use cases we have not yet established strong priors for what is 'normal'. Unfortunately, checking such points is time-consuming and underlying issues leading to the data error can change over time. An outlier detection approach should therefore be able to optimally use the knowledge gained from verification of the ground truth and adjust accordingly. With advances in machine learning, this can be achieved by applying reinforcement learning in a statistical outlier detection approach. The approach uses an ensemble of proven outlier detection methods in combination with a reinforcement learning approach to tune the coefficients of the ensemble with each additional bit of data.[11] Figure 6 plots the distributions of outlier scores for the three different methods in the ensemble. In a reinforcement learning approach, an algorithm is not just trained and applied but in each iteration the algorithm gets feedback on its performance. In this case, analysts manually check a set of extreme values identified by the algorithm and record their assessments. The algorithm then takes this feedback into account and presents a new list of outliers (possibly also incorporating fresh data).

[10] Nijhuis and Van Lelyveld (2023).

[11] Ensembles combine the strengths of different types of algorithms to get better performance.

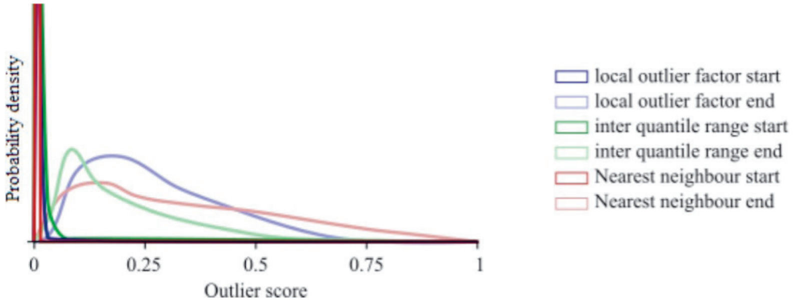


Figure 6: Outlier detection with reinforcement learning

This figure shows the distribution of the outlier scores for the first and last iteration for the different parts of the ensemble.

Source: DNB DSH project documentation.

At the Data Science Hub, we are currently implementing the reinforcement learning outlier detection approach using granular data reported by Dutch insurers and pension funds under the Solvency II and FTK frameworks. This application shows that outliers can be identified by the ensemble learner. Moreover, applying the reinforcement learner on top of the ensemble model can further improve the results by optimising the coefficients of the ensemble learner.

The second use case is KYC. KYC is a mandatory customer due diligence process that requires financial institutions to verify customer identity and assess and monitor their activities to prevent fraud. Since larger banks often have millions of clients and billions of financial transactions, data science has huge potential to help to monitor customers and identify potentially fraudulent transactions. In fact, it is already applied. For example, Anzo (Cambridge Semantics) provides flexible knowledge graphs that allow institutions to connect customer information from structured and unstructured data and thus provides a data-driven solution for KYC processes. Of course, the use of data science to monitor customers comes with additional challenges such as discussions on consumer trust in technology and privacy. However, as Elliott et al. stress, without integrated and innovative contributions from the industry resulting in improved services, it will be impossible to shape a path towards more substantial technological innovations.[12] Whereas financial institutions have to comply with KYC guidelines and regulations, supervisors are in charge

[12] Elliott et al. (2022).

of assessing whether they do so. Based on samples of client data from supervised entities, the Data Science Hub in cooperation with our colleagues in integrity supervision have therefore developed an outlier detection model to do risk assessments of these clients and map them with the risk classification of the supervised entity. With this model we were able to effectively select clients with abnormal transaction profiles. More specifically, we applied an Isolation Forest outlier detection algorithm to millions of profiles. Figure 7 shows a plot with outlier detection scores for bank clients plotted against two client characteristics. The results of the outlier detection model resulted in identification of new risks and efficiency gains since supervisors are now able to consider all transactions instead of considering small samples. The model and results have been shared with the supervised banks to ensure transparency. This example clearly shows that the real value of data science lies in the combination of the domain knowledge of the supervisor and the computational power of a computer to analyse millions of client transactions. The importance of domain knowledge is the topic of the next section.

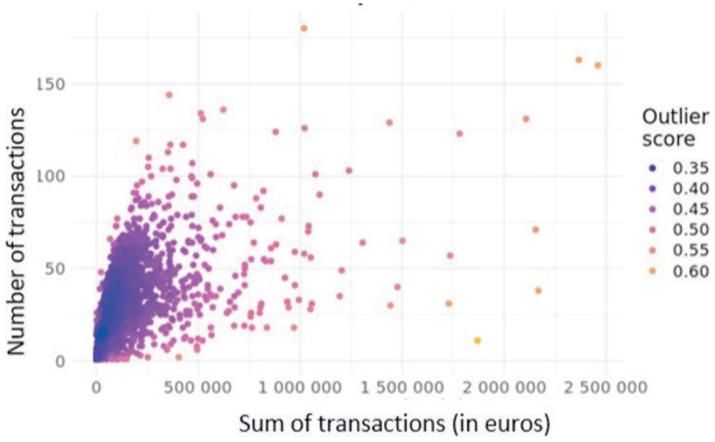


Figure 7: Using outlier detection for integrity risk

This figure shows a plot with outlier scores for bank clients plotted on two characteristics of those transactions, i.e. the sum of transactions (in euros) and the number of transactions by the client.

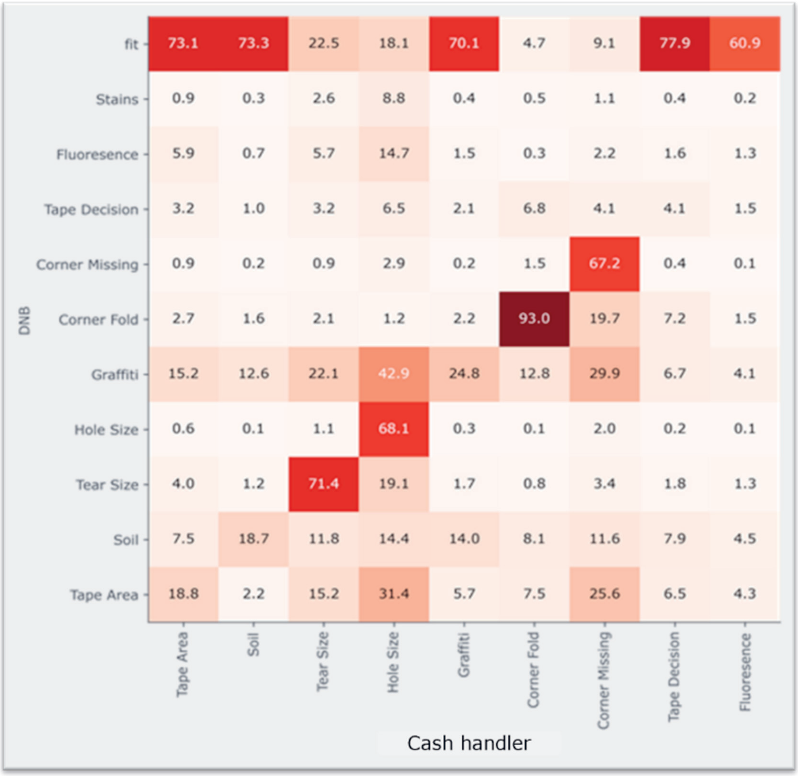
Source: DNB DSH project documentation.

2.5 Domain knowledge

As stated, the KYC project is a perfect example that shows the importance of domain knowledge in data science projects. This was also stressed by DNB board member Steven Maijoor in his speech at the Data Science Conference organised by the Data Science Hub in 2022 using the following example. To detect outliers in client transaction data, we traditionally define tell-tale identifiers. For example, 'multiple accounts on a single address' and 'a single deposit per month and immediate withdrawal.' Seen separately, these are relatively innocent. Together, however, they can indicate human trafficking of seasonal workers. The combination identifies subcontractors who organise housing for seasonal workers, which is a perfectly legal activity. But if at the same time there is an immediate withdrawal of the wages deposited with only a fraction of the wage paid to the worker it is clearly an illegal activity. However, the combination could also be consistent with student housing: a large inflow when student grants and loans arrive and a relatively quick withdrawal rate. While these examples are just based on two dimensions, in practice there are many more dimensions and these can interact in multiple and non-linear ways. With the use of data science techniques, we can identify them. Exactly for this reason data scientists should be in close contact with colleagues with domain knowledge, not only to provide input for the model but also to interpret model outcomes.

Another example of a data science project that shows the importance of domain knowledge is our False Unfit Banknotes project. Commercial cash handlers send banknotes that they consider unfit for circulation to DNB. Cash handlers also manage ATMs in the Netherlands. Unfit banknotes are checked again at DNB because DNB has specific authentication sensors to determine whether a banknote is unfit for circulation. During the sorting process at DNB, it appears that a large percentage of these unfit banknotes are still evaluated as fit. This is what we classify as 'false unfit.'

In cooperation with colleagues from the Payments division, the Data Science Hub investigated the high percentage of false unfit banknotes and how this percentage could be reduced. By looking at the data on the matched banknotes, it can be seen where the classification differs between DNB and the cash handler and specific rules that do not add up can be pinpointed. Figure 8 shows the percentage of cases in which DNB and the cash handler classifications are in line. For example, in 93% of the cases both DNB and the cash handler decide to classify a banknote as unfit due to a folded corner, and hence in 7% of the cases the cash handler decides to classify a banknote as unfit due to a folded corner while DNB does not. Hence, for fully compatible measurement, the diagonal of the matrix from the bottom left to the top right would be filled with dark squares, as the cash handler's trigger would be identical to the DNB's trigger. The number of DNB fit classifications if the cash handler detects a problem shows the extent of the false fit problem. Only the hole size, the tear size and the corner defects are regularly triggered for the same banknote by both the cash handler and DNB. The settings on the cash handler's machine could be adjusted to reduce the number of false unfits. While it is easy to compare the consequences of adjusting just one of the rules (e.g. tape decision or dirt), it quickly becomes more complicated once multiple rule settings are adjusted simultaneously. We therefore applied machine learning to arrive at the optimal combination of multiple rule adjustments. Reducing the number of unfits can save much effort and expense, and this project resulted in a set of recommendations for our Payments division to achieve these cost reductions.



	Tape Area	Soil	Tear Size	Hole Size	Graffiti	Corner Fold	Corner Missing	Tape Decision	Fluoresence
fit	73.1	73.3	22.5	18.1	70.1	4.7	9.1	77.9	60.9
Stains	0.9	0.3	2.6	8.8	0.4	0.5	1.1	0.4	0.2
Fluoresence	5.9	0.7	5.7	14.7	1.5	0.3	2.2	1.6	1.3
Tape Decision	3.2	1.0	3.2	6.5	2.1	6.8	4.1	4.1	1.5
Corner Missing	0.9	0.2	0.9	2.9	0.2	1.5	67.2	0.4	0.1
Corner Fold	2.7	1.6	2.1	1.2	2.2	93.0	19.7	7.2	1.5
Graffiti	15.2	12.6	22.1	42.9	24.8	12.8	29.9	6.7	4.1
Hole Size	0.6	0.1	1.1	68.1	0.3	0.1	2.0	0.2	0.1
Tear Size	4.0	1.2	71.4	19.1	1.7	0.8	3.4	1.8	1.3
Soil	7.5	18.7	11.8	14.4	14.0	8.1	11.6	7.9	4.5
Tape Area	18.8	2.2	15.2	31.4	5.7	7.5	25.6	6.5	4.3

Figure 8: Detecting False Unfit Banknotes

Source: DNB DSH project documentation.

2.6 Implementing data science

Note that the success of any algorithm is crucially dependent on how seamlessly we can integrate innovation in the existing workflow. We have seen countless promising proofs of concepts (PoCs) received with much enthusiasm that fail to make their way into production.

Note that the concept of 'in production' is a source of much confusion between IT and the average user. Typically, an analysis is used to set policy as soon as the policymaker is convinced that the results are solid. The analysis is often somewhat a journey and invariably involves manual steps. Reproducibility is often not the first concern and it is ensured because the analyst is closely involved and has intimate knowledge of how to replicate the results. For an IT department that is asked to bring such an analysis into production, the standards need to be much higher: the process needs to run without (much) manual intervention or knowledge of the subject matter. This involves programming to catch all kinds of eventualities and extensive unit testing. The challenge is to find an organisational form that allows abstracting away typical IT housekeeping tasks (e.g. ensuring proper backups) while allowing the analyst sufficient flexibility in further developing the tool.

In many cases, it has been too difficult to provide feedback to improve the algorithm since data science environments were kept too separate from what the average user could access or is comfortable with. In other cases, users underestimate the considerable effort that is needed to train and tune a model. Based on smooth experiences with consumer apps, they have unrealistic expectations of what bespoke algorithms can do in the short run.

2.7 Data science can add value anywhere in the organisation

The easiest place to begin the journey towards a data-driven organisation is to start with numerical information. Often, quantitative information is already available in databases close to where data scientists have tooling available. Early on in the transformation, our focus has been on automating manual steps in, for instance, risk assessments or forecasting exercises. Manipulation of such data now also touches on other less traditional topics. For example, we are experimenting with motion sensors in our office building to forecast how busy our cafeteria will be. Such forecasts can help our catering service plan capacity and our staff make a more informed choice to time their lunch.

Other departments that are now starting to get involved are ones that work mainly with text. A large amount of information flows into DNB as text. Natural language processing (NLP) and recent advances in large language models (LLMs) such as ChatGPT and BARD have great promise for data science applications in all parts of a central bank. One hurdle we face is that document storage and retrieval have not evolved at an equal pace. Documents are scattered in different systems, are not stored in a consistent format, and are difficult to access from our analytics platform. Notwithstanding these hurdles, we see more and more initiatives to make new data science techniques work for less traditional departments, such as, for example, our HR department.

References

Chakraborty C. and Joseph A. (2017). *Machine learning at central banks.* Bank of England Working Paper 674.

Elliott K., Coopamootoo K., Curran E., Ezhilchelvan P., Finnigan S., Horsfall D., Ma Z., Ng M., Spiliotopoulos T., Wu H. and Van Moorsel A. (2022). *Know your customer: balancing innovation and regulation for financial inclusion.* Data & Policy 4 (Oct. 2022).

Hüser A.-C. (2015). *Too Interconnected to Fail: A Survey of the Interbank Networks Literature.* Journal of Network Theory in Finance 1.

Hüser A.-C. and Kok K. (2019). *Mapping bank securities across euro area sectors: comparing funding and exposure networks.* ECB Working Paper 2273.

Jones D., Snider C., Nassehi A., Yon J. and Hicks B. (2020). *Characterising the Digital Twin: A systematic literature review.* CIRP Journal of Manufacturing Science and Technology (Mar. 2020).

Nasution M.K.M. (2020). *The birth of a science*. History of science and technology 10 (Dec. 2020). Number: 2, 315–338.

Nijhuis M. (2022). *Company Name Matching*. Medium.

Nijhuis M. and Van Lelyveld I. (2023). *Outlier Detection with Reinforcement Learning for Costly to Verify Data*. Entropy 25.

Rietveld G., Lange N. and Duijm P. (2023). *Measuring intra-bank complexity by (not) connecting the dots with LEI.* DNB Analyse.

Van Dijk D. and De Winter J. (2023). *Nowcasting GDP using tone-adjusted time varying news topics: Evidence from the financial press.* DNB Working Paper 766.

van den Boom B., Hofman R., Jansen K. and van Lelyveld I. (2021). *Estimating Initial Margins – The COVID-19 market stress as an application*. DNB Analysis.

4. Sandboxes and financial innovation facilitators[1]

Alain Otaegui Chapartegui
Policy Expert in Digital Finance at European Banking Authority

1. An overview of financial innovation facilitators in the EU

In the last decade, the competent authorities in the EU have adopted various initiatives to facilitate financial innovation. Many initiatives are designed to promote greater engagement between the authorities and the private sector on innovation with a view to, on the one hand, enhancing industry's understanding of regulatory and supervisory expectations and, on the other hand, increasing the authorities' knowledge of innovations, technologies and the opportunities and risks they may present.

To facilitate innovation the authorities use various tools, the most widespread being regulatory sandboxes and innovation hubs. This was clearly reflected in a joint report on regulatory sandboxes and innovation hubs[2] in January 2019 by the three European Supervisory Authorities (ESAs – EBA, ESMA and EIOPA). The report provided a good basis for understanding the

[1] The content of this chapter reflects the opinions of the author and does not necessarily reflect the views of EBA.

[2] JC ESAs (2019).

differences between the various types of innovation facilitators, mainly innovation hubs and regulatory sandboxes.

As was explained in the report, innovation hubs are dedicated points of contact within the competent authorities made available to private sector firms to raise enquiries with the authorities on fintech-related issues and to seek (non-binding) guidance on the conformity of innovative financial products, financial services and business models with licensing or registration requirements and regulatory and supervisory expectations. In turn, regulatory sandboxes are defined as competent authority-controlled environments that provide a way to enable firms to test innovative financial products, financial services and business models, following a specific testing plan agreed and monitored by a dedicated function of the competent authority.[3]

In addition, the 2019 report provided an extensive comparative analysis of existing innovation facilitators in the EU. At that time there were 21 innovation hubs and 5 regulatory sandboxes established in EU Member States and 3 hubs in EEA States. As is reflected in these numbers, a majority of States have established innovation hubs, with a smaller number having established regulatory sandboxes. In some, both forms of innovation facilitator have been implemented, and in others the hubs have preceded sandboxes. However, since the publication of the 2019 report a number of competent authorities have established additional hubs and sandboxes as a result of the good experiences of the authorities that have established one. For this reason, in December 2023 the ESAs published a new report on innovation facilitators[4] that provides an updated overview of the number of existing hubs and sandboxes. Additionally, the report examines the design and operation of innovation facilitators, observed practices in existing hubs and sandboxes, as well as challenges and limitations faced by competent authorities in operating them. Finally, the report sets out a series of considerations and recommendations for further enhancing the role of innovation facilitators and their effectiveness. Figure 1 and Figure 2 below show the competent authorities that have established innovation hubs and regulatory sandboxes respectively in EU and EEA countries, as reflected in the ESAs report.

[3] Sandboxes may also involve the use of legally provided discretion by the relevant supervisor (with use depending on the relevant applicable EU and national law) but they do not allow disapplication of regulatory requirements that must be applied as a result of EU law.

[4] JC ESAs (2023).

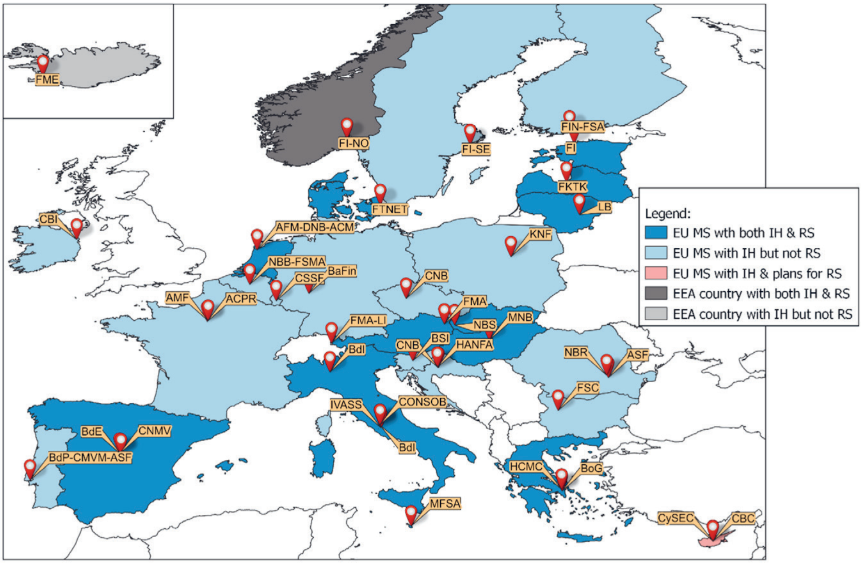


Figure 1: Financial sector innovation hubs in the EU / EEA (October 2023)
Source: JC ESAs (2023).

Since 2019, therefore, plenty of activity has been ongoing at the national and EU levels regarding innovation facilitators, with many financial sector authorities setting up new facilitators, mainly sandboxes, in their jurisdictions. As of October 2023, in the European financial sector there exist at least 41 innovation hubs and 14 regulatory sandboxes (see Figure 1 and Figure 2).

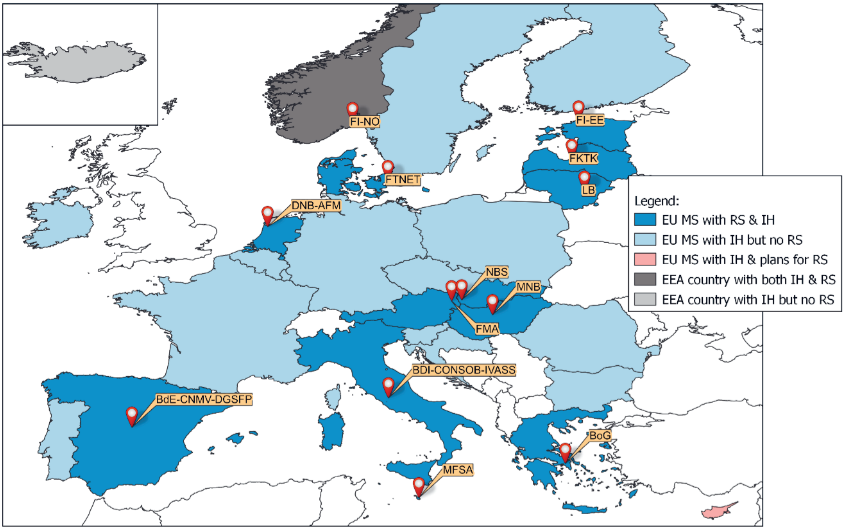


Figure 2: Financial sector regulatory sandboxes in the EU / EEA (October 2023)
Source: JC ESAs (2023).

This growing trend has been encouraged by the perceived benefits reported by the authorities that first set up sandboxes and hubs. Among the main benefits that have been identified are that they allow the authorities to gain a better understanding of innovation in financial services and help them develop a good understanding of potentially undue regulatory barriers against financial innovation. For example, in 2022 they were very successful in helping authorities improve their understanding of innovations related to so-called DeFi, NFTs and AI use cases in the financial sector. Innovation facilitators are also apparently allowing firms to better understand the regulatory and supervisory expectations that apply to the products, services and business models they might be developing or transforming on the basis of rapid technological advances or emerging technologies. As facilitators help improve the accessibility of authorities for firms, particularly for new entrants and technology providers, they provide a useful channel to get clarifications regarding regulatory and supervisory issues at an early stage in their innovation development and testing timeframes.

However, deploying innovation facilitators also introduces some challenges for authorities, in a context in which they might face difficulties finding and retaining staff with the appropriate knowledge and experience of fintech-related issues. In the case of regulatory sandboxes, a key challenge for authorities has been that some innovations tested in sandboxes may have been perceived by consumers and/or the market to have been 'endorsed' by the authority, resulting in either potential preferential access to financing and/or preferential market positioning. There are also legal and reputational risks for the authority if consumers suffer detriments as a result of services provided in the course of sandbox participation.

In addition, fintech players continue to put pressure on incumbent players and traditional business models in the financial sector. Therefore, policymakers need to keep track of market developments and assess whenever regulatory or supervisory actions are needed, both individually and jointly at the cross-sector and cross-border levels. To do this properly it is necessary to maintain a continual dialogue and close engagement between industry, supervisors, regulators and other stakeholders in the financial sector. This is essential for all parties to maximise the benefits brought to the EU financial sector by innovative applications. At the same time risks for consumers and investors are mitigated effectively.

In this context, in coordination with the European Commission and following recommendations in the 2019 report, the ESAs established a European

Forum for Innovation Facilitators (EFIF).[5] The EFIF provides a platform for supervisors with competences in fintech activities to regularly meet to share their experiences of engagement with firms through innovation facilitators. The EFIF also helps develop common views on the regulatory treatment of innovative products, services and business models, boosting coordination between supervisors on fintech topics. As a consequence, it can be said that the EFIF helps competent authorities and the ESAs to adopt a forward-looking response to regulatory and supervisory gaps in fintech, and promote greater cross-disciplinary coordination, knowledge-sharing and collaboration.

2. A cross-border testing framework for the EU financial sector

In addition to providing a platform for authorities for the aforementioned purposes, in December 2021 the EFIF developed and published a Cross-Border Testing Framework.[6] The objective of the framework was to enable and promote the sharing of testing-related information across borders in a structured manner and to facilitate the scaling up of innovative products and solutions, streamlining communication between authorities when a firm is interested in involving multiple authorities in testing. Additionally, the ESAs expect the framework to increase the accessibility of information and transparency on cross-border testing possibilities, and overall to reduce the limitations and challenges in the scaling of financial innovations across the EU.

The framework envisages three possible roles for supervisors: they can provide the regulatory sandbox; participate in the testing as observers; or just be recipients of test findings. Regarding the private sector, the framework is open to all types of companies. The key requirement is only that applying firms need to have first applied for testing in at least one regulatory sandbox in the EU. Qualifying firms can then submit a request for multi-sandbox testing, for observing sandbox testing or for sharing test findings.

In part to provide an interface for the cross-border testing framework developed by the ESAs, the European Commission set up an EU Digital Finance Platform,[7] which provides access to the cross-border testing tool. In addition,

[5] EBA European Banking Authority. *European Forum for Innovation Facilitators*. See here.

[6] EFIF (2021).

[7] EC European Commission. *EU Digital Finance Platform*. See here.

the platform offers a collaborative space for firms and authorities, including a Digital Finance Observatory that features an overview of the latest policy developments and research, events and calls to action, and an EFIF Gateway, which is a portal that provides updates on the work of the EFIF and information on how to contact relevant national authorities and find out about national licensing requirements.

While neither the platform nor the cross-border testing framework have gained the expected traction, the ESAs and the European Commission remain committed to offering the necessary tools to support the uptake and upscaling of fintech activities in the EU, including cross-border testing when firms deem it beneficial.

3. New types of approaches and tools in financial innovation facilitators

In addition to innovation hubs and regulatory sandboxes, the competent authorities in the EU have begun experimenting with new tools and activities to support innovation in the financial sector. The authorities have recognised that each innovation (depending on factors like the stage of development, scaling ambition, technology and governance) may be suitable for or require a different type of facilitation to upscale. That is, in order to overcome these challenges and find the best possible set-up to facilitate certain innovations, the authorities have become innovators themselves. They have done so in part because of increasing competition among themselves to attract innovators that can bring value to the fintech ecosystem of specific countries or regions. This can be observed from the fact that some innovative approaches adopted by EU authorities are inspired by ones employed by authorities in other countries, such as the Financial Conduct Authority in the UK and the Monetary Authority of Singapore.

While most of these emerging types of financial innovation facilitation activities have been recently identified and analysed by the IMF,[8] it may be useful to provide a general overview of the activities observed in the EU.

[8] IMF (2023).

First, an increasing number of authorities are setting up or organising digital or virtual sandboxes.[9] These aim to support testing based on a fully digital platform, and in most cases include providing access to synthetised publicly available datasets and to application programming interfaces (APIs) (provided by other firms or the authorities themselves) that give them access to data that is very useful (sometimes even necessary) in testing and otherwise unavailable to them. These types of sandboxes are most often used for use cases that assess the upscaling feasibility of a project, for instance to consider whether the cost of generating and using synthetic or anonymised data is worth the benefits brought by the solution. They are particularly useful to support innovations that require large data sets for testing purposes, such as those that use machine learning algorithms.

Second, other authorities have organised TechSprints,[10] which are short intensive events that bring together participants from financial services and outside them to develop technology-based ideas or proof of concepts to address specific challenges faced by regulators. When the focus of the event is heavily on coding and programming and the innovation mainly relies on them they are called hackathons. However, hackathons are typically organised by the private sector and not by the competent authorities. Nonetheless, the Monetary Authority of Singapore, for example, has organised what it calls 'hackcelerators,' with the 2023 edition dedicated to the use of artificial intelligence (AI) in finance.[11] These events normally bring together supervisors and staff from the competent authorities with computer programmers, interface designers, domain experts and technical staff from the private sector to intensively collaborate over a short time on a particular problem or use case. The objective is usually to solve or overcome a clearly delineated problem or innovation barrier set by the authority.

Third, a trend can be observed in which innovation facilitators are organised around thematic areas. Typically, in line with and to focus on pre-identified priority innovation areas at the national or authority level, an increasing number of authorities organise their facilitators by thematic areas, such as sus-

[9] See for example the Virtual Sandbox PSD2 to test solutions based on the Open API interface, and the Sandbox DLT ICT to provide an in-house-built DLT/Blockchain testing environment set up by the Polish Financial Supervision Authority (UKNF). Available here.

[10] In 2021, the ACPR in France ran a TechSprint on the topic of explainability of algorithms and black boxes (see here) and in 2022 launched another on the mutualisation of data on AML/CFT (see here).

[11] MAS (2023).

tainable finance, distributed ledger technology (DLT), AI and open finance.[12] This approach to sandboxes aims to align the authorities' own goals with the private sector's efforts with respect to the sandbox. It is a result of a recognition that authorities at times also have specific needs, be they understanding the functioning of a specific emerging technology or understanding the key features of an innovative business model. Being transparent about their goals and priorities helps firms put effort where support from authorities will be more useful (for the authority) and fosters innovation in areas of public interest. As a result, thematic areas may be particularly useful where the national or regional fintech ecosystem is mature enough to respond to such requests.

Finally, authorities are also demonstrating a forward-looking broad approach to facilitating financial innovation by organising industry roundtables,[13] fintech fora[14] [15] and workshops to improve engagement between authorities and industry representatives. Similarly, to improve collaboration between authorities themselves, different types of fintech networks and bridges have been set up.[16] These are expected to contribute to improving cross-border coordination, including on the testing of fintech use cases at the cross-border level.

[12] For instance, Banca d'Italia's FinTech Milano Hub launched its Call for proposals for 2022, with a focus on the use of DLT for banking, financial, insurance and payment services. See Banca d'Italia's website here.

[13] The Czech National Bank's Contact Point has organised regular meetings with the fintech community, having, for instance, organised in 2022 an industry roundtable focused on the use of machine learning in the Czech financial industry and the financial sector use cases covered by the AI Act. See CNB Czech National Bank.

[14] The Danish FSA has created a Fintech Forum, which gathers a wide range of sector representatives and the purpose of which is to establish an informal forum where the Danish FSA and the sector can discuss developments in the area of fintech. See Finanstilsynet.

[15] In Germany, BaFin has launched a 'FinTech Dialogue' in the context of its FinTech Forum to enable a systematic evaluation of incoming queries in order to identify relevant issues and address them in a target-oriented manner. See BaFin (2023).

[16] The Danish FSA has created a supervisory FinTech bridge with the Monetary Authority of Singapore (MAS). See MAS (2017).

4. Financial innovation facilitation in specific areas of the financial sector

So far, as has been described in this chapter, most innovation facilitators have been set up for the financial sector in general or for a specific sub-sector (banking, insurance or financial markets). However, the European Commission has recently begun to slightly adapt and innovate its approach to regulation in other areas affecting the financial sector by introducing experimental clauses or (voluntary or mandatory) development of regulatory sandboxes in legal acts.

An example of this is the AI Act, which based on the Commission's proposal[17] in April 2021 and the trilogue agreement announced by co-legislators on 9 December 2023[18], includes a whole chapter dedicated to promoting the creation of AI regulatory sandboxes to test AI systems in one or more EU Member States. The proposed framework requires competent national authorities to associate with other relevant regulators (e.g. data protection authorities, sectoral supervisory authorities) on the AI sandbox, and proposed that coordination and cooperation of all national AI sandboxes should be organised by a future EU AI Office, under which an AI Board composed of Member State representatives will be created. While the AI Act will not start applying in full until two years after its entry into force, Spain has already launched an AI regulatory sandbox, managed by the new Spanish Agency for the Supervision of AI (AESIA),[19] which will pilot and learn lessons for future AI sandboxes.

Similarly, but with a distinct approach, the DLT Pilot Regime Regulation[20] has provided the basis for the creation of national regulatory sandboxes to experiment with the use of DLT in market infrastructure for trading and settling transactions by financial instruments. This proposed act promotes the creation of a controlled environment to experiment with temporary exemptions from certain financial service rules (e.g. MiFID II, CSDR) to enable firms to test the application of DLT technology in trading and settling tokenised securities. The objective of this approach is to foster the development of innovative secondary markets for financial instruments in the EU and assess whether this requires future changes to the existing financial services legislation.

[17] See EC (2021) COM(2021) 206 final.

[18] Council of the EU (2023).

[19] See Government of Spain. Real Decreto 729/2023.

[20] See Regulation (EU) 2022/858.

Another initiative in this direction is the European Blockchain Regulatory Sandbox,[21] which has been established by the European Commission in coordination with the European Blockchain Services Infrastructure (EBSI). The objective of the new sandbox is to increase legal certainty for innovative blockchain technology solutions, and to provide legal advice on the operation of the core services of the EBSI and its use cases as approved by the European Blockchain Partnership (EBP). Use cases covered by the sandbox may include data portability, B2B data spaces, smart contracts and digital identity (including self-sovereign identity) in the health, environment, mobility, energy and other key sectors.

5. The outlook for innovation facilitators in the EU financial sector

Following a successful uptake of innovation facilitators in the EU, including in the financial sector but also in other sectors such as the energy and 'health-tech' sectors, the European Commission has identified, in particular regulatory, sandboxes as an emerging approach to policy assessment. This was reflected in the recent update of the European Commission's Better Regulation Toolbox,[22] in which it added a new Tool 69 on *Emerging methods and policy instruments*. Using this tool, the Commission contemplates different emerging policy approaches that Member States could follow to facilitate innovation at the national level. For instance, the Commission suggests they could draw up a list of existing experimentation tools in the policy field under consideration to identify potential friction between legislation and selected innovations. They could also issue guidelines in specific innovation fields to reduce regulatory uncertainty. These cases could avoid the need for sandboxes that typically provide temporary exemptions or allow for the testing of specific use cases.

However, at the same time, the Commission is finding many benefits of regulatory sandboxes in policy. Certainly, sandboxes can be useful to inform impact assessments and to estimate the impacts of different policy options affecting the regulatory environment. As the Commission has warned, however, when using sandboxes to inform impact assessments it is relevant to consider whether the indications provided by the sandbox results are applicable to the

[21] EC European Commission. *European blockchain regulatory sandbox for Distributed Ledger Technologies.*

[22] See EC European Commission. *Better Regulation Toolbox.*

innovation after it reaches a broad scale. Because the objective of facilitating innovation is also to support upscaling, it is of utmost importance to identify cases in which potential new risks and negative impacts are likely to derive from scaling-up or from EU-wide application.

In line with these findings and recommendations by the Commission, in addition to the ESAs' recommendations and considerations to NCAs, the Commission and the ESAs themselves, it remains relevant to assist national authorities in their support of the uptake of innovative applications across the EU.

In particular, there is an innovative approach to innovation testing that is being increasingly used by authorities all over the world and is being pushed for by the Commission: using synthetic data for testing. Synthetic data offers authorities the possibility to participate in testing a project without having to make real data they hold accessible to firms. In the financial sector, the creation of synthetic datasets for innovation testing has already been piloted by national authorities with the collaboration of the Commission. It was successfully tested in a pilot with the Bank of Spain and the results indicated that the synthetic data produced were accurate and privacy concerns were addressed. As a consequence of the successful experience, the Commission has recently complemented its Digital Finance Platform with a Data Hub[23], to give innovative firms access to synthetic supervisory data for the purpose of testing new solutions and training AI/ML models.

All in all, authorities in the EU are finding ways and themselves innovating to identify the most suitable approach to facilitate innovation in the financial sector, not only by adding new features to existing regulatory sandboxes and innovation hubs but also by organising new types of activities and events in collaboration with the private sector. In the end, the objective of all parties is to promote innovation in the EU, with authorities adapting their work to every type of innovation they come up with in the market.

[23] See here.

References

ACPR (2022a) Autorité de Contrôle Prudentiel et de Résolution. *ACPR Tech Sprint on the explainability of artificial intelligence – Summary Report*. January 2022. Available here.

ACPR (2022b) Autorité de Contrôle Prudentiel et de Résolution. *ACPR Tech Sprint on Confidential Data Pooling – Summary Report*. December 2022. Available here.

BaFin (2023) Bundesanstalt für Finanzdienstleistungsaufsicht. *Fintech Forum 2023*. Available here.

CNB Czech National Bank. *Financial innovation*. Available here.

Council of the EU (2023). *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*. December 2023. Available here.

EBA European Banking Authority. *European Forum for Innovation Facilitators.* Available here.

EC European Commission. *Better Regulation Toolbox – Tool #69. Emerging methods and policy instruments.* Available here.

EC European Commission. *EU Digital Finance Platform.* Available here.

EC European Commission. *European blockchain regulatory sandbox for Distributed Ledger Technologies.* Available here.

EC (2021) European Commission. *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.* COM(2021) 206 final.

EFIF (2021) European Forum for Innovation Facilitators. *Procedural Framework for Innovation Facilitators cross-border testing*. December 2021. Available here.

Finanstilsynet. *Fintech Forum*. Available here.

Government of Spain. *Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial.* BOE-A-2023-189112021/0106(COD), 2 September 2023. Available here.

IMF (2023) International Monetary Fund. *Institutional arrangements for fintech regulation: supervisory monitoring.* IMF Fintech Notes, June 2023. Available here.

JC ESAs (2019) Joint Committee of the European Supervisory Authorities. *Report on fintech: Regulatory sandboxes and innovation hubs*. JC 2018/74, January 2019. Available here.

JC ESAs (2023) Joint Committee of the European Supervisory Authorities. *Report on innovation facilitators*. JC 2023/27, December 2023. Available here.

MAS (2017) Monetary Authority of Singapore. *Monetary Authority of Singapore and the Danish Financial Supervisory Authority Signs fintech Agreement.* June 2017. Available here.

MAS (2023) Monetary Authority of Singapore. *MAS Launches AI in Finance Challenge for the 2023 Global fintech Hackcelerator.* June 2023. Available here.

Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU.

Section 3

Risks and Opportunities

1. Cyber risk and the financial sector[1]

Emran Islam
Senior Financial Sector Expert at International Monetary Fund

Klaus Löber
Chair CCP Supervisory Committee at European Securities and Markets Authority

In recent decades the global financial system has become more digitalised and interconnected. For it to function the real economy requires the financial system to reliably perform a range of key economic functions. These include payment services, securities trading, settlement services and deposit taking, among others. These processes have become increasingly digitalised, creating new and important interdependencies. Therefore, the financial system has come to critically rely on robust information and communication technology (ICT) infrastructure and the confidentiality, integrity and availability of data and systems. It follows that key economic functions can be disrupted by cyber incidents that affect the information systems and data of financial institutions and financial market infrastructures (FMIs).

The ability of attackers to undermine, disrupt and disable the ICT systems used by financial institutions is a threat to financial stability, one that requires additional attention. Attackers have broad access to technology, allowing them to operate across borders and to attack financial firms and central banks either for profit or simply to disrupt. An increase in the incidence of attacks, rising

[1] The contents of this chapter reflect the opinions of the individual authors and do not necessarily reflect the views of the IMF or the ESMA.

losses and recognition of the potential for serious disruption of the functioning of the financial system has raised cyber risk from an IT department concern to a central risk management issue for all financial institutions and a risk to system-wide stability. Attackers are universal in their reach – they target large and small institutions, rich countries and the less well-off alike.

Cyber risk is characterised by three key features that when combined fundamentally differentiate it from other sources of operational risk: the speed and scale of its propagation and the potential intent of threat actors. The interconnectedness of various information systems enables cyber incidents to spread quickly and widely. Some recent incidents[2] have demonstrated the ability of criminals to penetrate the networks of large organisations and quickly incapacitate them. Cyber incidents can also spread widely across sectors and beyond geographical borders, including to entities which are not the primary target of disruption. Malicious cyber incidents are becoming more persistent and prevalent, revealing the high level of sophistication and coordination that threat actors can achieve.

Financial systems are in varying states of readiness to manage such attacks, and the international response is fragmented.[3] Mitigating cyber risk in the financial sector is a key public policy objective. Digitalisation of the financial sector has led to even greater emphasis on cyber risk, which is now a priority for private financial institutions. Chief executive officers often cite this risk as one of their top three concerns. However, there is also clear public interest in managing cyber risk across the financial sector, especially since a successful cyber attack has the potential to jeopardise financial stability. Crucially, although financial institutions have clear individual incentives to invest in protection, without regulation and public policy intervention they will tend to underinvest from the perspective of society and the interests of the broader financial system. For example, they will not take into account the impact of their failure or of a broader attack on the system as a whole. While much is being done, we set out below the areas in which we see a need for further work, with emphasis on the role of the official sector.

We suggest there are six major building blocks that if created could considerably reduce cyber risk and help safeguard global financial stability. These build on the need to pay greater attention to prevention, mitigation, measurement and recovery. Addressing the building blocks will require a collaborative effort by standard-setting bodies, national regulators and industry associations,

[2] ESRB (2020).

[3] Adelmann et al. (2020).

and also by international financial institutions and other capacity development (CD) providers.

1. Cyber strategy

Authorities should develop a cyber strategy for their financial sector, integrating a number of key building blocks around regulation and supervision, sector resilience and public-private engagement and coordination. A cyber strategy can provide authorities with a clear vision and strategic objectives, with clarity on milestones, implementation plans, risk prioritisation and capacity building. Developing a cyber strategy entails working closely with other authorities and industry, building structures for collaboration and coordination, and helping to enhance the resilience of the entire sector.

2. Regulatory and supervisory frameworks

Cyber security regulation and supervision play important roles in strengthening resilience and delivering public policy objectives. Regulation and supervision set consistent minimum standards to be used by financial institutions, including promoting good cyber hygiene and setting expectations of risk management practices, incident reporting and response and recovery protocols, together with internal governance procedures. Active financial supervision supports effective implementation.

Good progress has been made in strengthening cybersecurity regulatory requirements, but fragmentation within and across borders causes inefficiencies. National requirements typically incorporate internationally recognised technical standards –requirements governing how to deal with the technology itself. However, there are currently often differences in the transposition[4] of the technical standards into national frameworks. While certain differences in requirements may be justified, fragmented control environments may complicate cyber risk management and drive compliance costs up, particularly for international financial institutions. Enhanced consistency and convergence among national and international approaches would free up resources that could be used more effectively to manage and respond to risk.

Efforts to address fragmentation and promote harmonisation are underway,

[4] Adelmann et al. (2020).

but convergence is a slow process. The Group of Seven (G7), the Financial Stability Board (FSB) and, jointly, the Committee on Payments and Market Infrastructure and the International Organization of Securities Commissions (CPMI-IOSCO) have published well-known high-level principles.[5] In practice, these guidelines have formed the basis for development of national standards for most of the larger and more sophisticated jurisdictions.

3. Financial stability analysis and cyber risk

Further improving identification of major sources of system-wide cyber risk and their potential impact on financial stability will strengthen risk mitigation. Cyber risk is now commonly highlighted in financial stability reports published by central banks and prudential authorities, although there is significant scope to improve both the quantification of risks and the integration of cyber risk in broader financial stability analysis. We outline below three such tools that could be widely adopted.

3.1 Cyber Mapping

A 'cyber map' identifies the main technologies, services and connections between financial sector institutions, service providers and in-house or third-party systems. At the conceptual level, mapping aims to highlight key financial and technological connections between financial institutions (including FMIs) and between these firms and third-party technology and service providers. Even a basic map will provide a valuable reference for supervisors to identify the key transmission channels through which cyber risk could become systemic, and the critical nodes and vulnerabilities in the system.

3.2 Quantitative Analysis

Accurate quantitative estimates of potential losses could usefully inform both firm risk management and financial stability analysis, although producing reliable estimates is difficult and remains work in progress. Difficulties stem in part from the limited availability of data on the frequency and loss severity of cyber attacks. Against this backdrop, improving the quality and availability of

[5] See G7 (2016), FSB (2020), and CPMI-IOSCO (2016).

data on losses from cyber attacks, and further developing modelling techniques would help support risk management, supplementing qualitative approaches that rely heavily on expert judgment. Being able to strengthen quantitative and qualitative analysis will allow authorities and financial entities to better understand the potential impact of a cyber incident on the system as a whole.

3.3 Stress Testing

Stress testing of cyber risk offers promise as a tool to support supervisors and policymakers. In such approaches, financial institutions are typically asked to assess the impact of cyberattacks on liquidity and capital. These tests generally involve institutions estimating losses in a prescribed scenario and a supervisory review of financial institutions' procedures and coverage against cyber security risk. Cyber risk scenarios can also be included in the stress testing and network analysis of FMIs. These exercises encourage financial institutions to further develop their risk management practices in this area. As an example, the IMF conducted a cyber risk surveillance of Singapore which included quantitative estimates of potential losses, among other matters. On average, banks estimated that losses from a direct cyber attack would amount to about 35-65 percent of their quarterly net profits depending on the cyber scenario type, and would cause the capital adequacy ratio (CAR) and the liquidity coverage ratio (LCR) to drop by 0.1-0.4 and 8.4-35 percentage points respectively. [6]

Comparatively, cyber risk quantification at the systemic level is in an earlier stage of development. This is an active area of financial stability analysis. Although there are large uncertainty margins around current estimates, they are likely to narrow as data and modelling approaches continue to improve. Estimates of potential losses are high. For example, Monte Carlo simulations estimate the 95 percent value at risk (VaR) loss to be $147 billion for financial institutions globally (14 percent of global net income). In a further experiment the mean cyber attack frequency is set at double its historical peak. In this scenario, the 95 percent VaR loss rises to $352 billion (34 percent of net income).[7]

[6] Goh et al. (2020).

[7] Bouveret (2018).

4. Response and recovery — Cyber resilience

Cyber resilience has emerged as an important concept in cyber security. While strong cyber hygiene and preventative actions remain important, past assumptions that cyber attacks can be repelled or are relatively rare have given way to the reality that such attacks are a continuous threat and that many will have a degree of success. As the sheer number of incidents rises, both industry and supervisors have refocused from zero tolerance of successful breaches of institution systems toward a more pragmatic approach that concentrates on containing the problem and maintaining operations.

The industry and regulators are enhancing their capabilities to take action after a detected cybersecurity incident (response function) and to restore any impaired systems or services (recovery function). Financial institutions are strengthening internal response and recovery protocols that help maintain critical business functions during disruptions. Such preparations also reduce the incentives for those seeking to disrupt operations. In addition, supervisors have started developing protocols that take an industry-wide view of critical financial services to ensure that operations are maintained or can recover quickly to avoid undue disruption. Supervisors play a key coordination role in responses. They are uniquely positioned to identify and observe incidents across financial institutions, are able to share information broadly across the sector in a timely manner and play a critical role in restoring and maintaining public confidence, including through communication.

Strengthening the cross-border aspects of response and recovery arrangements is a top priority. Financial institutions are often connected across borders – through parent institutions, subsidiaries, counterparties in other jurisdictions, correspondent banks and FMIs – and their ability to respond to and recover from attacks may rely on conditions or actions taken across borders.

Cyber security exercises are very effective resilience assessment tools for financial institutions and supervisors alike. These exercises are planned events during which an organisation simulates a cyber attack that disrupts operations and tests capabilities (for example, prevention, detection, mitigation and response and recovery). An extension is ‘red-teaming,’ which is designed to help entities test and improve their resilience against cyber attacks by employing actual hacker methods to breach or circumvent defences. Cyber security exercises can identify gaps in the operational resilience of institutions and financial systems, helping to identify priorities that strengthen response and recovery capabilities. Exercises can also point to gaps in information sharing arrangements and support collective action to address them, whilst red team testing frameworks driven by authorities (e.g. TIBER-EU,[8] CBEST[9] etc.) can strengthen the protection, detection and response capabilities of financial institutions.

5. Information sharing

Information is the lifeblood of risk mitigation and is the basis for risk management and supervisory frameworks. Pooling information on cyber risks can enhance situational awareness, help detect new risks and build better responses. Sharing information also reduces the cost of collection for all participants, including in the financial sector.

There are currently, however, significant barriers to sharing – most importantly regulatory barriers and concerns about liability. Limitations on information sharing, particularly across borders, can increase vulnerabilities because information silos can be exploited by cyber attackers, who are able to work across jurisdictions with ease.

Information sharing in the realm of cybersecurity includes the following:

- Threat intelligence information – information on the source and nature of threats, including on which groups may be targeting a specific set of institutions, the technology being targeted or used and the intention behind the attacks. Threat intelligence information can also include high-frequency alerts, risk analytics, indicators, threat assessments and analysis. This information gives financial institutions and supervisors a basis for monitoring and addressing vulnerabilities. Such information varies in depth and specificity and is typically shared on a continuous basis between trusted sources.

- Incident reporting – information on the success of the incident and how it was addressed. It may include loss information. Supervisors usually require reporting of incidents with an account of how the financial institution is managing the situation.

[8] See here.

[9] See here.

- Good practices – information on how cyber incidents are reported and analysed, what incident response was made and what the consequences have been. Good practices also extend to how resilience is being built in institutions in the financial system and how the supervisor is addressing the risk.
- Defence techniques – information on how an attack was prevented or contained, which may be shared at the technical level.

There are three broad channels of information sharing in the financial sector, and they are at different levels of maturity:

- Private sector institution to private sector institution – the sharing of cybersecurity threat intelligence information between financial institutions in domestic financial sectors is well advanced in many financial systems, including among large global institutions. Sharing may be on an informal basis, such as through personal relationships between chief information security officers, or on a more formal basis. Information is typically shared on a continuous basis in a trusted network and is highly valuable given its relevance to risk managers.
- Private sector institution to public agency – private financial institutions typically provide their supervisors with incident reports. Routine protocols for regulatory reporting together with trusting relationships between supervisors and institutions help support this exchange.
- Public sector to public sector agencies – financial supervisors may share incident reports and regulatory responses with other domestic agencies or with cross-border peers. Examples typically include sharing incident information between home and host supervisors.

Promoting trusted information sharing among private and public institutions can help overcome resistance. Platforms where threat intelligence is shared on a continual basis establish efficient and long-standing relationships that build trust. For example, the Financial Services Information Sharing and Analysis Centre (FS-ISAC) has developed a network for central banks, regulators and supervisory authorities (the CERES Forum) for members to receive timely targeted information, tools and resources about cybersecurity threats and threat mitigation strategies. Other examples of international arrangements for information sharing include those in place as part of the Euro Cyber Resilience Board for pan-European Financial Infrastructures' (ECRB's) Cyber Information and Intelligence Sharing Initiative (CIISI-EU).

6. Deterring cyber threats

Cyberattacks are a global phenomenon that presents significant challenges to law enforcement, especially at the international level. The constant rapid evolution of hacking technologies makes policing, prosecution, sanctioning and asset recovery work difficult, even though there has been some success.

International agreement on addressing cyber attacks is a politically sensitive topic. The 2001 Budapest Convention[10] is the only binding multilateral agreement aimed at combating cyber crime. Offences under the convention include (1) offences against the confidentiality, integrity and availability of computer data and systems; (2) computer-related offences; (3) content-related offences; and (4) criminal copyright infringement. In November 2019 a United Nations cyber crime resolution set up a drafting group to establish terms of reference for a new global cyber crime treaty. The international constituency is divided, however, over fears of criminalising ordinary online activities by individuals and organisations through cyber crime laws.

Cyber attacks generate a significant amount of illegal proceeds every year in advanced and developing economies alike. Although cyber attacks may be committed for a range of motives (for example, political, competition, cyber war ones), many are profit-driven. Some studies estimate that ransomware incidents alone generate some $1 billion in illegal proceeds every year.[11] Developing economies face huge challenges as attackers exploit underinvestment in defences and may even use these economies as testing grounds for new techniques. The proliferation of digital currencies, which, when unregulated, provide anonymity and make it difficult if not impossible to trace the beneficiary owner or end receiver of funds makes it easier to generate and launder the proceeds of crime. In this context, effective implementation of a comprehensive anti-money laundering and combating the financing of terrorism (AML/CFT) framework in all countries is crucial. In particular, requirements that private sector firms such as banks identify their customers, maintain relevant records, monitor transactions and report suspicious transactions to the relevant authority are essential to prevent and combat cyber crime and the laundering of its proceeds. Sound AML/CFT frameworks also help with the recovery of the illegal proceeds of cyber crime.

[10] See Budapest Convention, available here.

[11] McGuire (2018).

Cyber attacks should be made both expensive and risky through effective measures to seize and confiscate the proceeds of crime, and also to identify and sanction criminals. Success in this respect is predicated on effective international cooperation. That is, information sharing and formal mutual legal assistance. Otherwise, cyber criminals simply shift operations to jurisdictions that do not cooperate effectively.

7. Conclusion

In an increasingly interconnected and digitalised global economy, cyber risk continues to be at the top of most risk categories. Tackling cyber risk requires a coordinated approach built on a holistic strategy, and effective regulation and supervision, financial stability analysis, response and recovery, information sharing and cyber deterrence. All of these require close coordination and collaboration between authorities and the financial industry.

References

Accenture (2019). *Ninth Annual Cost of Cybercrime Study*. Conducted by Ponemon Institute, Traverse City, MI.

Adelmann F., Elliott J.A., Ergen I., Gaidosch T., Jenkinson N., Khiaonarong T., Morozova A., Schwarz N. and Wilson C. (2020). *Cyber Risk and Financial Stability: It's a Small World After All*. IMF Staff Discussion Note, International Monetary Fund, Washington, DC.

Adelmann F. and Gaidosch T. (2020). *Cybersecurity of Remote Work during the Pandemic*. IMF Special Series on COVID-19, International Monetary Fund, Washington, DC.

Aldasoro I., Gambacorta L., Giudici P. and Leach T. (2020). *Operational and Cyber Risks in the Financial Sector*. Bank for International Settlements Working Paper 840, Basel.

Bank of England (2018). *Could a cyber attack cause a systemic impact in the financial sector?*. Quarterly Bulletin, 2018 Q4.

Barrett B. (2019). *The Catch-22 That Broke the Internet*. Wired, June 7.

BIS (2008) Bank for International Settlements. *The Interdependencies of Payment and Settlement Systems*. Basel.

BIS (2018) Bank for International Settlements. *Cyber-resilience: Range of Practices*. Basel.

BIS and IOSCO (2014) Bank for International Settlements and International Organization of Securities Commissions. *Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers*. Basel.

Boer M. and Vasquez J. (2017). *Cyber Security and Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System*. Institute of International Finance, Washington, DC.

Bouveret A. (2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*. IMF Working Paper 18/143, International Monetary Fund, Washington, DC.

Cambridge Centre for Risk Studies (2014). *Sybil Logic Bomb Cyber Catastrophe Scenario*.

Carnegie Endowment for International Peace (2017). *Timeline of Cyber Incidents Involving Financial Institutions*. Washington, DC.

CPMI (2018) Committee on Payments and Market Infrastructures. *Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security*. Bank for International Settlements, Basel.

CPMI-IOSCO (2016) Committee on Payments and Market Infrastructures, and International Organization of Securities Commissions. *Guidance on Cyber Resilience for Financial Market Infrastructures*. Bank for International Settlements, Basel. Available here.

CPSS (2012) Committee on Payment and Settlement Systems, Technical Committee of the International Organization of Securities Commissions. *Principles for Financial Market Infrastructures*. Bank for International Settlements, Basel.

Danielsson J., Fouché M. and Macrae R. (2016). *Cyber risk as systemic risk*.

Doffman Z. (2019). *Cybercrime: 25% of All Malware Targets Financial Services, Credit Card Fraud up 200%*. Forbes, 29 April 2019.

ECB (2018a) European Central Bank. *Cyber Resilience Oversight Expectations for Financial Market Infrastructures*. Frankfurt.

ECB (2018b) European Central Bank. *TIBER-EU framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*.

ECB (2019) European Central Bank. *ECB Banking Supervision: Risk Assessment for 2019*.

Eisenbach M., Kovner A. and Lee M. J. (2020). *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis.* Federal Reserve Bank of New York Staff Report 909.

ESRB (2020) European Systemic Risk Board. *Systemic Cyber Risk*.

FSB (2018) Financial Stability Board. *Cyber Lexicon*. Basel.

FSB (2019a) Financial Stability Board. *Cyber Incident Response and Recovery*. Progress report to the G20 finance ministers and central bank governors meeting in Fukuoka, Japan, June 8-9, 2019.

FSB (2019b) Financial Stability Board. *Third-party Dependencies in Cloud Services: Considerations on Financial Stability Implications*. Basel.

FSB (2020) Financial Stability Board. *Effective Practices for Cyber Incident Response and Recovery*. Basel. Available here.

Gaidosch T., Adelmann F., Morozova A. and Wilson C. (2019). *Cybersecurity Risk Supervision*. IMF Departmental Paper 19/15, International Monetary Fund, Washington, DC.

Goh J., Heedon K., Koh Z.H., Lim J.W., Ng C.W., Sher G. and Yao C. (2020). *Cyber Risk Surveillance: A Case Study of Singapore*. IMF Working Paper 20/28, International Monetary Fund, Washington, DC.

Gray A. (2017). *Credit Data Groups Face More Scrutiny after Equifax Hack*. Financial Times, 11 October 2017.

G7 (2016) Group of Seven. *G-7 Fundamental Elements of Cybersecurity for the Financial Sector*. ECB. Available here.

G7 (2016) Group of Seven. *G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*. Taormina, Italy.

Healey J., Mosser P., Rosen K. and Tache A. (2018a). *The future of financial stability and cyber risk*. Brookings Institution.

Healey J., Mosser P., Rosen K. and Wortman A. (2018b). *The Ties That Bind: A Framework to Assess the Linkage Between Cyber Risks and Financial Stability*. CRFS Working Paper.

Heijmans R. and Wendt F. (2020). *Measuring the Impact of a Failing Participant in Payment Systems*. IMF Working Paper 20/81, International Monetary Fund, Washington, DC.

Institute of International Finance (2017). *Cyber Security and Financial Stability: How Cyberattacks Could Materially Impact the Global Financial System*.

IMF (2020) International Monetary Fund. *Norway: Financial Sector Assessment Program–Technical Note–Cybersecurity Risk Supervision and Oversight*. IMF Staff Country Report 2020/262, Washington, DC.

(ISC)2. (2019). *Cybersecurity Workforce Study*. Clearwater, FL.

Kashyap A. and Wetherilt A. (2019). *Some Principles for Regulating Cyber Risk*. AEA Papers and Proceedings, 109:482-487.

Kopp E., Kaffenberger L. and Wilson C. (2017). *Cyber Risk, Market Failures and Financial Stability*. IMF Working Paper No 17/185.

LaVito A. (2017). *Equifax Security and Information Executives to Retire*. CNBC report, 15 September 2017.

Lipton D. (2020). *Cybersecurity Threats Call for a Global Response*. Blog. International Monetary Fund, 13 January 2020.

McGuire M. (2018). *Into the Web of Profit*. Cupertino, CA: Bromium.

NBB (2018) National Bank of Belgium. *The Financial Market Infrastructures and Payment Services Report*. Brussels.

NBB (2019) National Bank of Belgium. *The Financial Market Infrastructures and Payment Services Report*. Brussels.

Office of Financial Research (2017). *Cybersecurity and Financial Stability: Risks and Resilience*. Washington, DC.

UN (2019) United Nations Human Rights Council. *Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*. New York.

World Economic Forum (2016). *Understanding Systemic Cyber Risk*. White Paper.

2. Fintech and green fintech – Digital innovation for the SDGs and climate agenda

Katherine Foster
Executive Director at The Green Digital Finance Alliance

1. Introduction

This chapter delves into the evolution of the SDGs and the climate agenda, and focuses on the promise and challenges of digital technology in advancing these global goals. It provides definitions of key concepts such as digital technology, the fourth industrial revolution, fintech and green fintech, and highlights their significance in the context of the climate and sustainable development goals (SDGs) together with the challenges involved. The chapter addresses the need for integrative approaches, pathways and governance to promote inclusive sustainable financial practices and investments in climate and SDG solutions.

2. Evolution of the sustainable development goals and the climate agenda

The Sustainable Development Goals (SDGs) were adopted by all the United Nations Member States in 2015 as a universal call to action to end poverty, protect the planet and ensure that all people enjoy peace and prosperity by

2030.[1] In the same year, the Paris Agreement established a comprehensive framework aimed at averting climate change while emphasising the responsibility of developed nations to provide financial resources to aid developing countries in addressing climate change impacts.[2] These two global frameworks marked a turning point in setting national and international goals and targets for climate and sustainable development.

However, the journey towards achieving these sustainable development and climate goals began over three decades ago at the United Nations Conference on Environment and Development – also known as the Rio Conference.[3] Rio highlighted the interdependence of various social, economic and environmental factors, and emphasised that progress in one sector requires action in other sectors.[4]

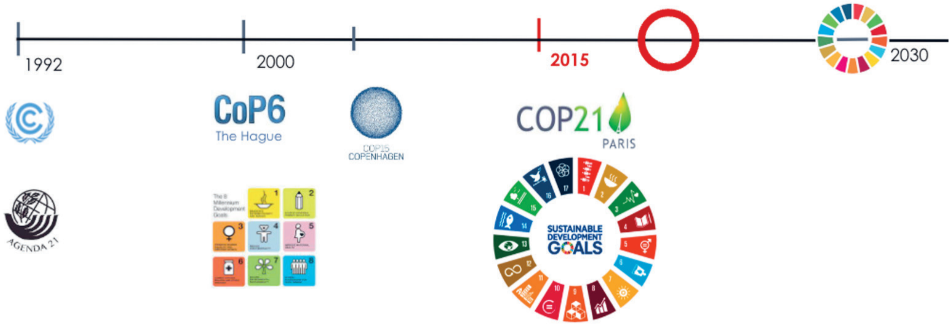


Figure 1

Source: the author (2023)

The primary outcome of Rio was an integrated agenda on environmental and development issues "that would help guide international cooperation and development policy in the twenty-first century."[5] Agenda 21 was a blueprint for sustainable development action to be taken at the local, national and global

[1] UN United Nations. *The Sustainable Development Goals.*

[2] UN Climate Change. *The Paris Agreement.*

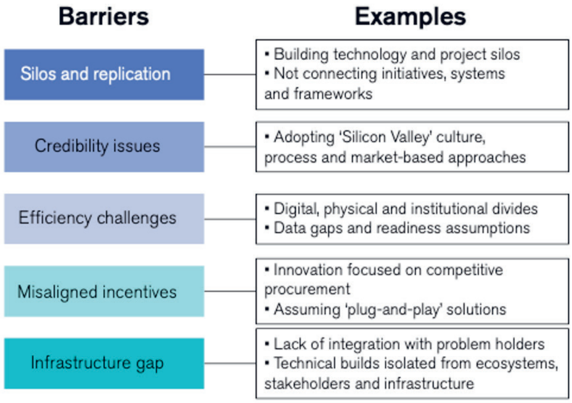
[3] Rio built on the foundation laid by the United Nations Conference on the Human Environment in 1972 in Stockholm, which marked the first global recognition of environmental issues linked directly to development. See UN United Nations. *1972 United Nations Conference on the Human Environment*.

[4] UN Climate Change. *The Rio Conventions.*

[5] Ibid.

levels. It was then iterated through the 2000 Millennial Development Goals and climate protocols and conventions through to the Paris Agreement and the SDGs in 2015.

Despite Rio's focus on integrated action, solutions for climate and sustainability evolved in a fragmented manner. By 2015, the solution space had evolved to one fraught with issues of replication, infrastructure gaps, credibility, data deficiencies and monitoring and reporting complexities.[6]



Barriers	Examples
Silos and replication	• Building technology and project silos • Not connecting initiatives, systems and frameworks
Credibility issues	• Adopting 'Silicon Valley' culture, process and market-based approaches
Efficiency challenges	• Digital, physical and institutional divides • Data gaps and readiness assumptions
Misaligned incentives	• Innovation focused on competitive procurement • Assuming 'plug-and-play' solutions
Infrastructure gap	• Lack of integration with problem holders • Technical builds isolated from ecosystems, stakeholders and infrastructure

© Katherine Foster (2018)

Figure 2

Source: Foster and Nassiry (2021)

The 2015 SDGs encompassed 17 goals and 169 corresponding targets across environmental, economic, social and governance themes,[7] proposing a balanced and comprehensive approach to sustainable development. All 193 United Nations Member States committed to work towards these goals by setting and measuring progress towards their own commitments. The Paris Agreement combined legally binding international commitments with nationally determined contributions (NDCs) based on each country's circumstances and capabilities.[8] As such, the mechanisms related to climate and sustainability goals launched in 2015 relied largely on countries self-regulating and reporting.

Translating the SDGs and the Paris Agreement into actionable measurable initiatives for non-state actors such as corporations and financial institu-

[6] Foster and Nassiry (2021).

[7] UN United Nations. *The Sustainable Development Goals.*

[8] UN Climate Change. *The Paris Agreement.*

tions likewise involved mainly non-binding mechanisms. These included collaborative and voluntary contributions to national climate actions, reporting platforms and financial support. While these mechanisms and national and international regulatory frameworks continue to evolve, measuring progress towards commitments and targets remains a substantial challenge for all stakeholders – from national governments to local NGOs to financial institutions.

3. The promise of digital revolutions to address the fragmented solution space

The timing of the Paris Agreement and the SDGs aligned with an international focus on digital and emerging technology and the narrative of the fourth industrial revolution. The narrative brought a general sense of optimism around the capacity of emerging and digital technologies to help bridge the gaps in reaching the goals of the new agreements and to address the challenges and complexity of measuring progress and impacts.[9] The fourth industrial revolution was even integrated in the policy dialogue and initiatives in the United Nations system.[10]

The focus was not only on the capacity of digital and emerging technology to drive efficient and innovative solutions across the SDGs (including climate) but in the actual financing of the SDGs, as was illustrated by the UN Task Force on Digital Financing of the SDGs established in 2018.[11] The convergence of digital and emerging technology and finance presented a unique opportunity to address climate change, facilitate efficient and accessible financial inclusion, foster equitable growth and unlock financing for impact solutions.

[9] World Economic Forum (2020).

[10] UN United Nations (2020).

[11] UN United Nations. *The Task Force on Digital Financing of the Sustainable Development Goals.*

Key terms such as digital technology, emerging technology and fintech are constantly evolving. Defining and delineating these in the context of this chapter is important to understand their contextual variations and the opportunities and challenges they bring, including governance considerations. For the purpose of this chapter, the following definitions are adopted.

Digital technology refers to a broad range of tools, systems and applications that use digital information and communication technologies to perform various tasks and functions. It encompasses hardware, software and networks that enable the processing, storage and transmission of digital data. Examples of digital technologies include computers, smartphones, the internet, cloud computing, artificial intelligence, blockchain and the internet of things.[12]

Emerging technology refers to innovations in the nascent stages of development or adoption, often involving advances across or within existing technologies with potential for substantial impacts. Emerging technologies frequently bring about profound social, institutional or economic changes and address challenges like climate change and sustainable development.[13] As such they are held up as critical drivers of progress.

Digital innovation involves the use of emerging and integrated digital technologies to create new products, services and business models to enhance efficiency, productivity and competitiveness. Additionally, it is situated to address complex global issues, including climate change, poverty and inequality and is lauded for its capacity to drive new types of economic and social development and to facilitate novel forms of communication and collaboration.[14]

The fourth industrial revolution. Emerging digital technologies and innovations overlap and are noted for their potential to disrupt industries, enhance efficiency, improve customer and user experiences, and address complex challenges such as climate change and sustainable development.[15]

[12] OECD (2019).

[13] World Economic Forum (2019a). *Global Technology Governance: A Multistakeholder Approach*.

[14] World Economic Forum (2019b). *Unlocking Technology for the Global Goals*.

[15] World Economic Forum. *The Fourth Industrial Revolution.*

> This narrative – which was popularised in 2016 by Klaus Schwab, the founder and executive chair of the World Economic Forum – emphasises the role of technology in fundamentally shifting industrial capitalism. The narrative was also applied to how emerging technologies, such as artificial intelligence, the internet of things, big data, fintech and blockchain, could be harnessed to address pressing global environmental, economic and social issues.[16]

The legacy of fragmented innovation continued in the siloed approach to digital technology for the SDGs and climate solutions, including how the financial sector addresses these global challenges.

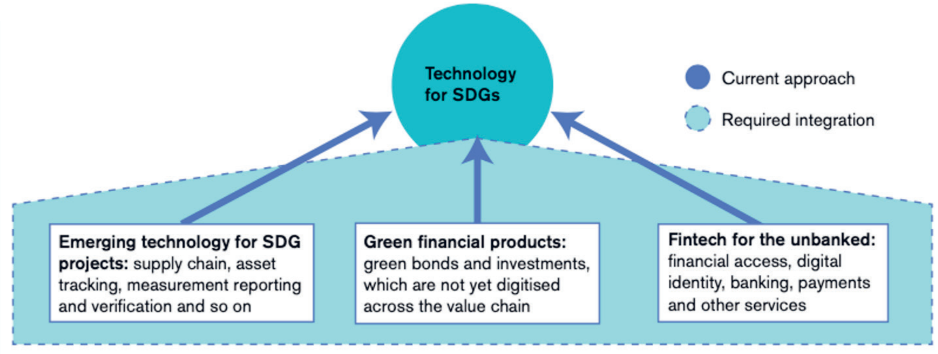

Technology for SDGs
● Current approach
○ Required integration
Emerging technology for SDG projects: supply chain, asset tracking, measurement reporting and verification and so on
Green financial products: green bonds and investments, which are not yet digitised across the value chain
Fintech for the unbanked: financial access, digital identity, banking, payments and other services

Figure 3: Emerging technology for SDG landscape

Source: Foster and Nassiry (2021).

Within the financial sector, the SDGs are predominantly viewed through the lens of environmental, social and governance (ESG) factors, which financial institutions and corporations use to report on climate and sustainability practices. ESG frameworks enable investors to evaluate the risk, the sustainability and ethical impact of investments. Digital innovation in different sectors enhances the capacity to address and report on ESG issues and to offer ESG-focused products.

[16] World Economic Forum (2019). *Globalization 4.0: Shaping a New Global Architecture in the Age of the Fourth Industrial Revolution*. Available here.

4. Fintech

Digital innovations in and related to the financial sector generally fall under the umbrella term ‘fintech’ – which is short for financial technology and encompasses a wide range of digital innovations transforming the financial sector.[17] These innovations include digital banking, mobile payments, cryptocurrency, peer-to-peer lending and robo-advisors, among others.[18] Financial entities like banks, investment firms, brokerages, lenders, insurance companies and credit card companies are embracing digital innovation in solutions aligned with the SDGs. These range from green bonds and climate-focused insurance products to digital accounts and lending services for underserved populations, including support for economic activities such as smallholder farming.

In addition, fintech includes instruments that address barriers in green investing and market accessibility together with resource-intensive processes. It streamlines issuance, facilitates asset aggregation, offers traceable digital instruments, enables real-time monitoring and AI-driven portfolio management, and promotes regulatory cooperation.[19] Fintech democratises access to financial services and empowers individuals and businesses to conduct transactions, manage investments and access credit without traditional intermediaries.[20]

Fintech further bridges the inclusion gap with innovations like mobile money and preloaded cards, enhancing convenience and accessibility. Stablecoins, community currencies and alternative digital assets further reduce the cost barriers associated with financial services.[21] Fintech also fosters gender equality by providing digital identities and alternative credit scoring models that consider non-traditional assets and behaviours, thus empowering women economically. Women's engagement in economic activities such as sustainable farming contributes to achieving multiple SDGs, including climate resilience, sustainable land use and food security. Fintech promotes financial inclusion, reduces poverty, promotes gender equality, stimulates economic growth, supports sustainable economic and environmental initiatives and infrastructure development, reduces inequalities and enhances institutional transparency.[22]

[17] Feyen et al. (2021).

[18] Ibid.

[19] Foster et al. (2021a).

[20] Blakstad and Allen (2018).

[21] Sahay et al. (2020).

[22] Ibid.

While fintech enhances the capacity of institutions to serve marginalised and underserved populations, the digital divide remains a significant challenge.[23] Approximately a billion people globally lack access to mobile phones and a third of the global population cannot access the internet, with women disproportionately affected.[24] Factors such as low population density, conflicts impacting communication infrastructure, a lack of electricity, harsh climatic conditions and the high cost of data contribute to this digital disparity. Inclusive technology design is imperative to promote economic equity and contribute to sustainable development on a global scale.

5. Green fintech: the intersection of digital innovation, ESG factors and the SDGs

In the dynamic world of fintech, the concept of green fintech has emerged as a subcategory encompassing digital technology and innovation focused on enabling environmental, social and governance (ESG) considerations in financial decision-making and advancing broader SDG solutions.

The Green Digital Finance Alliance (GDFA) has identified three waves of green fintech innovation.[25] The first wave involves digitising existing financial products and services to enhance inclusivity and accessibility. The second wave focuses on leveraging data to create innovative financial products, such as programmable utility tokens and fractional ownership of assets, with sustainability objectives. The third wave centres on using data and digital capabilities to develop entirely new financial products aligned with sustainability goals, while also improving the efficiency and reliability of existing green financial products. These solutions encompass digital platforms for green investment, carbon offsetting, sustainable supply chain management and energy-efficient financing with additional SDG impacts.

Green fintech has evolved from promoting sustainability in the financial sector to a range of activities, including climate risk assessment tools, advances in monitoring, reporting and verification of investment impacts, and directly unlocking funding for sustainability projects. It represents a promising area for innovation and investment, fostering new business opportunities and mobilising private capital for sustainable development goals.[26]

[23] Foster et al. (2021a).

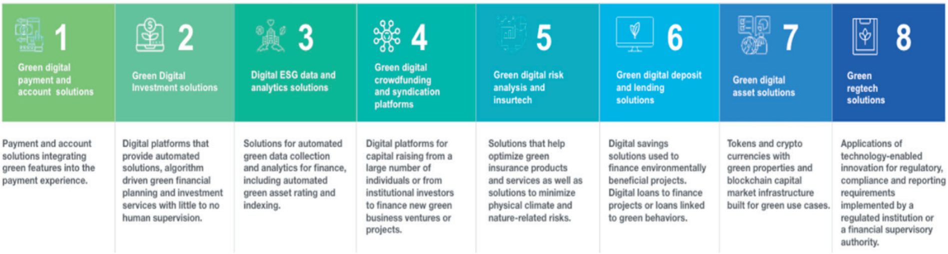
[24] Ibid.

[25] Green Digital Finance Alliance (2022).

[26] Green Digital Finance Alliance (2022).

According to GDFA, green fintech refers to financial technology solutions that support sustainable development.[27] GDFA delineates eight categories of green fintech solutions that combine financial innovation, digital technology and sustainability principles to support the transition to a low-carbon economy. Green fintech solutions can encourage green financing, responsible investment, environmental risk management and sustainable consumption. GDFA also highlights the importance of the databases utilised by each category and categorises them in four primary types: earth observation data; self-reported asset data through the IoT; registry and company data; and science and policy databases. These distinctions help underscore the crucial role of data in shaping and advancing the green fintech landscape.

6. Green Fintech Classification



1 Green digital payment and account solutions	2 Green Digital Investment solutions	3 Digital ESG data and analytics solutions	4 Green digital crowdfunding and syndication platforms	5 Green digital risk analysis and insurtech	6 Green digital deposit and lending solutions	7 Green digital asset solutions	8 Green regtech solutions
Payment and account solutions integrating green features into the payment experience.	Digital platforms that provide automated solutions, algorithm driven green financial planning and investment services with little to no human supervision.	Solutions for automated green data collection and analytics for finance, including automated green asset rating and indexing.	Digital platforms for capital raising from a large number of individuals or from institutional investors to finance new green business ventures or projects.	Solutions that help optimize green insurance products and services as well as solutions to minimize physical climate and nature-related risks.	Digital savings solutions used to finance environmentally beneficial projects. Digital loans to finance projects or loans linked to green behaviors.	Tokens and crypto currencies with green properties and blockchain capital market infrastructure built for green use cases.	Applications of technology-enabled innovation for regulatory, compliance and reporting requirements implemented by a regulated institution or a financial supervisory authority.

Figure 4

Source: Green Digital Finance Alliance (2022).

This categorisation was originally developed by GDFA in the context of the Swiss ecosystem with an intention for it to be globally applicable. However, it is essential to leverage it in a descriptive rather than prescriptive manner as green fintech is evolving to encompass additional contextual iterations and impacts across the SDGs, including those outlined in the fintech section.

7. Challenges, risks and recommendations

While the integration of digital products in finance holds significant promise for the SDGs and the climate agenda, it also presents several challenges and risks that need careful consideration. A notable overarching challenge is to develop innovation in separate silos, encompassing technology for financial in-

[27] Ibid.

novation, green and climate innovation, and broader SDG initiatives ranging from economic development to gender inclusion. Bridging these divides and aligning on terminology, capacity and data needs is essential to effectively leverage technology to address the climate and SDG agenda. This requires an integrative approach that entails not only technological solutions but also collaborative efforts across industries and sectors to maximise impact.

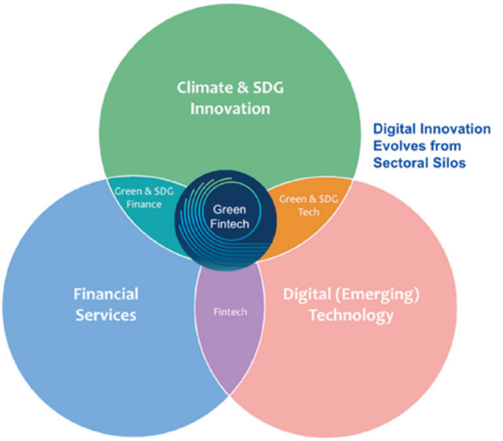


Figure 5: Green Fintech: Convergence of Digital Innovation Silos

Source: the author (2023)

The global nature of digital finance intertwined with the involvement of multinational corporations amplifies the complexity of cross-border coordination in regulatory oversight, taxation and data sharing, given the diversity of regulatory environments.[28] In addition to these overarching concerns, specific challenges spanning technical, ethical and regulatory dimensions warrant further examination.

[28] Foster et al. (2021a).

The digital divide is a persistent challenge, with a significant proportion of the global population lacking access to technology and the internet. If not approached thoughtfully, digital innovation can exacerbate existing inequalities further hindering digital finance solutions reaching vulnerable and underserved populations.[29] Ensuring that fintech and green fintech solutions are accessible and beneficial to all, including marginalised groups and developing economies, is crucial to drive sustainable and equitable growth.

Governments and international organisations should prioritise bridging the digital divide through infrastructure investment, digital literacy promotion, affordable technology and internet access to enable underserved populations to benefit from digital financial services and to foster inclusive growth. Furthermore, governments should promote and encourage green fintech innovation and development through incentives, grants and partnerships to drive green investments and sustainable development.

Expanding access means expanding reliance on digital platforms, which introduces new dynamics and risks. The extensive generation of data by digital platforms and services raises significant data privacy and security concerns. Ethical questions related to consent, data ownership and the potential for biased algorithms are especially pertinent in developing countries as access expands and the collection and utilisation of user data grows.[30] Ethical considerations in data and AI usage must be addressed through regulatory guidelines emphasising algorithmic transparency and bias mitigation and enhancing data literacy.

With expanded access, cross border integration and amplified data generation, the potential for cyber attacks, technical glitches, and operational disruptions also increases. This increases the risk of potential negative system impacts and risks for individuals if not adequately managed. Protecting individuals' sensitive financial and personal information is paramount to maintain trust in these systems.[31] Governments and regulatory bodies should enforce robust data protection, cybersecurity regulations and capacity building, empower individuals with data ownership rights and promote transparency in data usage.

[29] Foster et al. (2021b).

[30] Foster et al. (2021a).

[31] Foster et al. (2021b).

Another pressing issue relates to the growing demand for sustainable financial products, which carries an inherent risk of ‘greenwashing,’ in which products are inadequately vetted or measured, potentially undermining the overall credibility of green financial initiatives. This challenge accentuates the importance of establishing clear standards and transparency in sustainable finance. Collaboration among financial institutions, governments and international bodies is essential to set clear criteria for sustainable financial products to ensure reliable information for consumers. Cross-border cooperation is vital to ensure consistent and fair market practices.

"The future is digital, defining how we will live, work and interact with each other. Whether technology becomes an empowering force for good or a sower of more division and exclusion will depend on the choices we make now." Achim Steiner, UNDP Administrator during his address at the First Regular Session of the UNDP Executive Board 2023.

Balancing data-driven innovation and ethical and governance considerations remains a formidable challenge in this evolving multifaceted landscape. Regulatory authorities should adopt agile approaches that keep pace with technological advances while striking a balance between fostering innovation and safeguarding individual data and interests. Moreover, it is essential to include diverse stakeholders – civil society, NGOs, academia, industry and governments – to ensure a more inclusive design not only for governance frameworks but also agile support mechanisms. Mechanisms to enable continual learning and adaptation, such as ongoing assessment, review and adjustment of policies, are also imperative to enable regulator capabilities and governance in the rapidly evolving digital finance landscape. Addressing these multifaceted challenges necessitates a collective capacity building effort.

8. Conclusion

The convergence of digital technology and finance offers unprecedented potential to drive sustainable development and transform economies. Digital innovation has augmented efficiencies and services, has presented opportunities to address ESG issues in the financial sector and has unlocked innovation pathways to address and finance climate goals and the SDGs. In so doing, it has, however, introduced new challenges that necessitate careful consideration and responsive and collaborative governance.

The journey toward leveraging digital innovation – green fintech – for the SDGs holds promise but brings additional complexity. As technology evolves, policymakers, industry players and international organisations must collaborate to harness the benefits of digital innovation while mitigating risks, including those not covered by conventional policy and measurement frameworks. Fostering an innovation ecosystem that upholds ethical standards, respects data privacy and remains committed to sustainability principles is essential to the journey.

Enhancing regulator capabilities, fostering innovation, promoting financial inclusion and helping navigate the challenges and opportunities of digital finance are essential to leverage green fintech and ensure equitable and sustainable outcomes in a increasingly interconnected digital finance landscape. By establishing robust yet agile regulatory mechanisms, encouraging responsible and collaborative innovation and prioritising financial services aligned with the SDGs, governments and stakeholders can shape a future in which green fintech contributes to a more sustainable and inclusive global economy.

References

Blakstad S. and Allen R. (2018). *FinTech Revolution: Universal Inclusion in the New Financial Ecosystem*. Illustrated edition. Springer International Publishing.

Feyen E., Frost J., Gambacorta L., Natarajan H. and Saal M. (2021). *Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy*. BIS Papers No. 117. Monetary and Economic Department. Available here.

Foster K., Blakstad S., Bos M., Gazi S., Melkun C. and Shapiro B. (2021a). *Big-Fintechs and Their Impacts on Sustainable Development.* Technical Paper 1-1. UNDP-UNCDF-TP-1-1. Available here.

Foster K., Blakstad S., Bos M., Gazi S., Melkun C. and Shapiro B. (2021b). *BigFintechs and Their Impacts on Sustainable Development* Technical Paper 1-1 Annexes 1-6. Available here.

Foster K. and Nassiry D. (2021). *Digital technologies for an inclusive, low-carbon future that puts people first*. IIED, London, pg. 2. Available here.

Green Digital Finance Alliance (2022). *Green Fintech Classification*. Available here.

OECD (2019) Organisation for Economic Co-operation and Development. *Measuring the Digital Transformation: A Roadmap for the Future*, OECD Publishing, Paris. Available here.

Sahay R., Eriksson von Allmen U., Lahreche A., Khera P., Ogawa S., Bazarbash M. and Beaton K. (2020). *The Promise of Fintech: Financial Inclusion in the Post COVID-19 Era*. IMF Departmental Papers / Policy Papers 2020/009, International Monetary Fund.

UN (2020) United Nations. *Blockchain applications in the United Nations system: towards a state of readiness*. Available here.

UN United Nations. *The Sustainable Development Goals*. Available here.

UN United Nations. *1972 United Nations Conference on the Human Environment*. Available here.

UN United Nations. *The Task Force on Digital Financing of the Sustainable Development Goals*. Available here.

UN Climate Change. *The Paris Agreement*. Available here.

UN Climate Change. *The Rio Conventions*. Available here.

World Economic Forum (2019a). *Global Technology Governance: A Multi-stakeholder Approach*. Available here.

World Economic Forum (2019b). *Unlocking Technology for the Global Goals*. Available here.

World Economic Forum (2020). *Fourth Industrial Revolution Tech Can Fast Track 70% of Sustainable Development Goals*. News Releases. 16 January 2020. Available here.

World Economic Forum. *The Fourth Industrial Revolution*. Available here.

3. SupTech[1]

Claudia Guagliano
Head of unit, Consumer, Sustainability and Innovation analysis at European Securities and Markets Authority

Valentina Mejdahl
Risk analyst, Consumer, Sustainability and Innovation analysis at European Securities and Markets Authority

1. What is SupTech and how the concept emerged and evolved in the context of financial services

SupTech, short for supervisory technology, refers to the use of digital tools and solutions by regulators and supervisors with the aim of enhancing the effectiveness and efficiency of their supervisory activities in the financial industry. These SupTech solutions encompass a wide range of innovative technologies, including big data analytics, artificial intelligence (AI), machine learning (ML), natural language processing (NLP), cloud computing, application programming interfaces (APIs) and even natural language generation (NLG) and distributed ledger technology (DLT). These technologies are used to support various regulatory and supervisory activities that increasingly require to process and analyse large amounts of data.

SupTech covers a variety of activities ranging from simple digitalisation and

[1] The content of this chapter reflects the opinions of the individual authors and does not necessarily reflect the views of ESMA.

automation of internal administrative supervisory processes and interactions with supervised entities to crucial supervisory core activities. These core activities include data collection and analysis, market surveillance, anomaly detection, identification of suspicious activities, regulatory reporting and transparency, risk assessment, stress testing, systemic risk analysis, enforcement and handling complaints. Through automation, real-time data analysis and anomaly and pattern detection, SupTech assists regulatory authorities in identifying potential risks, detecting fraudulent activities and ensuring compliance in a more timely, accurate and cost-effective manner.

Overall, SupTech aims to enhance the quality of financial regulation and oversight, reduce regulatory burdens and costs, and increase transparency and trust in the financial system.[2]

The term 'SupTech' has emerged relatively recently in the context of financial regulation and supervisory practices and has gained prominence in the past decade. It evolved as an extension of the broader 'fintech' (financial technology) concept, specifically identifying the adoption of technology by supervisory authorities, which have increasingly transformed their oversight processes in the industry.

This transformation has been driven by various factors on the demand and supply sides. On the demand side there has been an increase in the volume and complexity of regulations developed in response to the 2008 financial crisis. This has necessitated the adoption of technology to effectively navigate and enforce compliance with these regulations. In addition, there has been a shift towards more data-driven supervisory processes, requiring larger amounts of data with greater granularity. Furthermore, there is an ongoing drive for efficiencies and cost reduction in supervisory activities, which has prompted the exploration and implementation of SupTech solutions.

On the supply side there have been significant technological advances in areas such as AI, big data analytics, cloud computing and ML. These advances have provided the necessary tools and infrastructure to support the development and deployment of SupTech solutions. Moreover, the growing availability of extensive volumes of financial data, both structured and unstructured, has offered regulators and supervisors a wealth of information for analysis and decision-making. Finally, the decreased costs of ICT software and hardware,

[2] Note that the concept of SupTech is often closely associated with RegTech, or regulatory technology, which focuses on the use of technologies by regulated entities to meet regulatory requirements and enhance compliance processes. SupTech and RegTech are interconnected as they both aim to leverage technology to enhance regulatory processes and achieve regulatory objectives. The focus of this chapter is on SupTech and how it helps enhance supervisory tasks. The following chapter in the e-book discusses RegTech.

computing power and storage have made it more affordable for regulatory authorities to adopt and leverage SupTech solutions.

These demand and supply drivers, coupled with recognition of the benefits offered by SupTech, have played a pivotal role in its development and adoption by regulatory authorities and supervisors.

Developments related to data in regulatory and supervisory practices have been instrumental in the emergence of SupTech. The availability of vast amounts of data, combined with advancements in data analytics and processing capabilities, has unlocked new possibilities for regulators and supervisors to leverage technology for enhanced oversight. Improved abilities to collect, store, manage and analyse data have served as catalysts for the development of SupTech solutions specifically designed to address critical tasks such as risk assessment, monitoring and compliance oversight. Data has such significance in SupTech that experts often identify two primary areas of SupTech application: data collection and data analysis.

While the use of technology in supervision is not new, and supervisory authorities have employed various solutions over the years to improve the efficiency of their processes and activities, the emergence of the SupTech concept marks a significant shift from the manual and fragmented approaches of data management and supervision to more automated, streamlined, faster and smarter supervisory processes.

Since around 2017, international standard-setting organisations such as the BIS, FSB, IMF, OECD and the World Bank have begun to operate with the term 'SupTech' while acknowledging and promoting its significance in strengthening supervisory practices. Reports and publications from these organisations[3] have highlighted the potential of SupTech to enhance data collection, analysis, risk monitoring and compliance oversight.

At the EU level, one of the first strategic documents that recognised the importance of technology in supporting better public services was the Digital Single Market Strategy for Europe, published in 2015.[4] Later in 2018, the European Commission adopted a FinTech Action Plan[5] outlining the ways to harness the opportunities presented by technology-enabled innovation in financial services. It emphasised a need to raise the level of regulatory and supervisory capacity and knowledge about new technologies.

[3] See for example BIS (2018), World Bank (2018), Lagarde (2018), FSB (2020), Denis (2021) and OECD (2021).

[4] See EC (2015) COM(2015) 192 final.

[5] See EC (2018) COM(2018) 109 final.

The Fintech Action Plan also called for the creation of an expert group to assess the presence of regulatory obstacles to financial innovation in the financial service regulatory framework. In 2019, the expert group on Regulatory Obstacles to Financial Innovation (ROFIEG) produced a report[6] discussing emerging opportunities for SupTech for the first time. The report called for support for advanced SupTech adoption by the financial sector, including enhancement of standardisation, use of a machine-readable common language and interoperability enabling the development of SupTech.

More recently, the EU Digital Finance Strategy,[7] published by the European Commission in September 2020, further developed the ideas of the FinTech Action Plan and set priorities to embrace digital finance for the benefit of consumers and businesses while mitigating the risks posed by the digital transformation. The Strategy defined SupTech as "a sub-set of FinTech that uses innovative technology to support supervision. It helps supervisory authorities to digitise reporting and regulatory processes."[8] Moreover, the strategy announced that the EU will aim to put in place the necessary conditions by 2024 to enable the use of innovative technologies, including RegTech and SupTech tools, for supervisory reporting by regulated entities and supervision by authorities. It stressed the importance of promoting data sharing between supervisory authorities.

Another prominent document that employs and promotes the concept of SupTech in EU financial services is the Supervisory Data Strategy adopted in 2021.[9] It refers to SupTech as one of the tools to modernise EU supervisory reporting and put in place a system that delivers accurate, consistent and timely data to supervisory authorities at the EU and national levels while minimising the aggregate reporting burden for all relevant parties.

In the context of national experiences with SupTech in Europe, there is a noticeable increase in SupTech activities by national competent authorities (NCAs). These activities predominantly revolve around data analysis, data visualisation, knowledge management with the use of ML and NLP tools. Conduct supervision, consumer protection and market abuse are among the most common areas of application of SupTech. Supervisors are also mindful of possible uses of SupTech tools across the entire data lifecycle, covering func-

[6] EC (2019).

[7] See EC (2020) COM(2020) 591 final.

[8] Ibid., p.13.

[9] See EC (2021) COM(2021) 798 final.

tions like data validation, conducting plausibility checks and data processing. Overall, efficiency and effectiveness are considered the most evident benefits of SupTech.

However, several substantial challenges impede broader development and adoption of SupTech solutions by NCAs. These challenges mainly involve data quality and resource limitations, including skill shortages and resource availability. Additionally, there are challenges related to ensuring transparency in supervisory decision-making processes, technological complexity, preparing all stakeholders involved in the supervisory process for the integration of SupTech and complying with the provisions of the General Data Protection Regulation (GDPR).

Regarding the evolution of the SupTech concept and the development and uptake of SupTech tools in Europe, it is important to discuss the role of the European Supervisory Authorities (ESAs): the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA), which have all recognised the importance of technology in enhancing supervisory practices and have actively promoted the adoption of SupTech in the European Union.

2. The ESAs' adoption and promotion of SupTech tools

The ESAs are the European-level financial regulators responsible for overseeing the banking, insurance and securities market sectors. Recognising the importance of technology in enhancing supervisory and regulatory practices, the ESAs have approached the realm of SupTech from three distinct yet interconnected directions.

First, the ESAs actively monitor developments in SupTech, as they do with other technologies and financial innovations. This ongoing monitoring allows them to ensure comprehensive understanding, identification and mitigation of risks associated with technological innovation in the finance industry. By conducting targeted surveys, exchanging information with industry stakeholders, academics, retail investor associations, fintechs, competent authorities and other EU and international organisations, the ESAs can identify emerging risks and provide guidance on areas where further work by European or national authorities may be necessary. For instance, ESMA has been monitoring and analysing SupTech's implications for securities markets and has published several analytical pieces on the topic.[10]

Second, the ESAs have made significant progress in transforming their own supervisory practices and processes to enhance efficiency through the adoption of SupTech tools. For example, ESMA has developed text-processing tools and employed NLP techniques and text-mining methods to support supervisory assessments. ESMA experts have also used data analytics techniques on large datasets, including AI/ML tools, to tackle various analytical challenges and have implemented machine learning-based systems for identifying abnormal data patterns. A case study of one of ESMA's NLP projects is provided in chapter 6 of this Section of the e-book. Other ESAs have also experimented with some of the new technologies and their application in supervision, like a social media monitoring tool which employs NLP technologies to assess market sentiment.

Last, the ESAs play a crucial role in actively promoting and facilitating supervisory convergence among national supervisory authorities, with an increasing focus on the use of digital technologies and SupTech tools. The ESAs support the adoption of SupTech by national authorities through exchanging knowledge and experience, sharing best practices, undertaking joint projects and fostering the development of skills and expertise. The ESAs have organised workshops, conferences and working groups to promote dialogue and exchange best practices. Moreover, the ESAs are actively exploring the potential for developing supervisory tools at their central level and ensuring their accessibility by national authorities. By fostering collaboration, the ESAs aim to create a supportive ecosystem for the development and adoption of SupTech tools across Europe.

[10] See ESMA (2019b), ESMA (2021a), ESMA (2021b) and ESMA (2022a).

Some ESAs have enshrined their SupTech-related objectives in their strategic documents. For example, in 2020 EIOPA adopted a SupTech Strategy[11] that explained the concept of SupTech, analysed then-existing SupTech practices at EIOPA and in national authorities and set up priorities for further SupTech projects. These priorities focused on promoting the exchange of knowledge and experiences between NCAs and with EIOPA and even sharing code/algorithms. The strategy also emphasised a need for improved data collection and analytics.

ESMA, in turn, has adopted a Data Strategy for 2023-2028[12] with the ambition for ESMA to become a reference point on RegTech/SupTech for NCAs, international regulatory and supervisory authorities, and the broader financial sector. The strategy sets an objective to use RegTech and SupTech solutions to consolidate and analyse multiple sources of data, including unstructured data, to make the use of data more effective and efficient.

The ESAs' proactive approach to SupTech has paved the way to a better understanding of its benefits and challenges, also by national authorities. By actively monitoring SupTech developments and promoting supervisory convergence, the ESAs ensure a comprehensive view of the associated risks and provide guidance to European and national authorities. In the next paragraph, we provide an overview of the benefits and challenges involved in SupTech adoption, building on ESMA’s experience.

3. NLP adoption by ESMA: benefits and challenges

As discussed in the previous paragraph, in recent years the ESAs have adopted some SupTech solutions applicable to their own supervisory practices and processes. Notably, ESMA has adopted NLP-based tools in several analytical projects related to supervision, market monitoring and risk analysis. Several key projects are briefly described below to exemplify the trend, focusing both on the advantages found and the challenges encountered in this technological transition.

[11] EIOPA (2020).

[12] ESMA (2023a).

In the first pilot project conducted in 2020, ESMA analysts applied NLP techniques to a dataset of over 54,000 key information documents (KIDs).[13] The aim of the exercise was to illustrate how NLP tools can assist supervisors in extracting pertinent information from a large set of regulatory documents. NLP tools provide new possibilities and measures for regulatory compliance assessment, enhanced risk analyses and decision-making and, ultimately, reinforced investor protection.[14] The use of NLP in this project allowed a diverse range of insights from the PRIIPs KIDs to be extracted (e.g. certain words or phrases, cost-related figures, simulated returns under different performance scenarios, summary risk indicators) that then enabled measurement of the completeness and complexity of the KIDs and conducting sentiment analysis. In fact, the information extracted from the texts was transformed into data for statistical analysis allowing trends and patterns to be identified.

While the benefits of NLP deployment in KID-related supervisory, analytical and policy tasks were clearly illustrated by this project, certain technical challenges were also evidenced. The first challenge relates to the structural format of the documents subjected to natural language processing. KIDs are almost always only provided in PDF format, necessitating conversion into machine-readable formats for NLP operations. The conversion process is lengthy, prone to error and may alter the outcome of the analysis. Undertaking this supplementary conversion task, which could be avoided if issuers generated KIDs in open document format, further revealed the importance of fostering the production of regulatory documentation – by both regulators and market participants – in a machine-readable format. This would allow further uptake of NLP and other SupTech tools, in line with the overarching trend towards digitisation.[15]

Another technical challenge revealed by the project consisted in the design and calibration of an algorithm capable of comprehensively addressing differences across documents written in multiple languages and styles to mitigate potential biases. This exercise, often involving expert judgment to extract objec-

[13] KIDs are produced under the Packaged Retail Investment and Insurance-Based Products (PRIIPs) Regulation with the purpose of informing retail investors when they are considering purchasing a PRIIP.

[14] See ESMA (2021b).

[15] A noteworthy development in this regard are the provisions of the recently adopted Regulation (EU) 2023/1114 , which require making crypto-asset white papers [art.6(10), art.19(9), art.51(9)] and some information published by crypto-asset service providers [art. 68(7)] available in machine readable format.

tive information from texts, further stressed the significance of human review and oversight in the presence of technology-facilitated processes. NLP techniques can support supervisors and provide complementary tools but should not replace human decision-making. It also highlighted the importance of relying on algorithms that are interpretable and can be reviewed in each step.

In 2022, ESMA conducted a similar project with the use of NLP techniques, focusing on prospectuses issued for securities like shares and bonds, and on how these prospectuses comply with the requirements of the EU Prospectus Regulation.[16] The exercise involved evaluating 593,000 pages of text (over 3,000 prospectuses) to create a comprehensive snapshot of the prospectuses considered and determine whether issuers across the EU are meeting the expectations of the legislators who designed the Prospectus Regulation. NLP techniques spotlighted shortcomings in the quality of information in prospectuses (e.g. broken hyperlinks, repetition, imprecise risk factors) and showed that longer prospectuses contribute to a greater divergence among rating agency assessments of credit risk. The study once again underscored the effectiveness of text-mining as a supervisory technology tool. Similar to the PRIIPs KIDs project, challenges were encountered in this study. First, constraints related to the PDF format of the documents submitted to the Prospectus Register affected text-mining. Second, biases needed to be mitigated when designing an algorithm and making choices of linguistic metrics, terms and analytical criteria. This challenge was addressed with increased transparency about the criteria selected and enhanced interpretability.

In 2022 and 2023, ESMA conducted two more projects leveraging NLP and focusing on environmental, social and governance (ESG) topics. In one of the projects ESMA experts applied NLP techniques to a dataset of over 64,000 press releases produced by credit-rating agencies (CRAs) to assess how they disclose information about the integration of ESG factors in their credit ratings.[17] The results of this assessment informed ESMA's work in the area of CRA supervision and risk analysis, revealing significant divergencies in CRA disclosures in terms of both CRA and ESG factors despite the fact that the overall level of ESG disclosures in CRA press releases has increased since the introduction of the 2019 ESMA Guidelines.[18] Once again, the study demonstrated that text-mining can extract information relevant for regulators from

[16] See ESMA (2022b).

[17] See ESMA (2022a).

[18] See ESMA (2019a).

large texts and documents that would otherwise have been intractable. The familiar challenges of document format transformation persisted, emphasising the need for machine-readable documents.

A more recent ESMA undertaking focused on assessing ESG names and claims in the EU investment fund industry with the aim of identifying and addressing risks of 'greenwashing.'[19] In this project NLP techniques were applied to a novel dataset with historical information on 36,000 funds, including regulatory documentation and marketing material. This exercise allowed evolving fund practices to be assessed and concluded that funds increasingly use ESG-related language in their names; that funds with ESG-related language in their name provide more extensive ESG disclosures and that funds sold to retail investors are associated with more extensive ESG language in key investor information documents (KIIDs)/KIDs compared with funds sold to institutional investors. In this project ESMA experts conducted the largest sustainability-related NLP assessment of EU fund documentation to date. The project further demonstrated that NLP-based tools have the potential to greatly assist effective supervision across the EU and more specifically can help recognise and counter the risks of 'greenwashing.'

4. Conclusions

SupTech is a crucial advance in the finance industry leveraging innovative technologies to enhance regulatory and supervisory activities. Its evolution has been driven by the increasing complexity of regulations, data-driven processes and the pursuit of efficiency and cost reduction in supervisory activities.

The emergence of SupTech represents a shift from manual and fragmented approaches to more automated, streamlined and efficient supervisory processes. International organisations, EU institutions and national supervisors have recognised the potential and significance of SupTech to strengthen supervisory practices.

The ESAs have made significant progress in monitoring and promoting convergence in national SupTech-related practices while transforming their own supervisory processes to enhance efficiency by adopting SupTech tools.

ESMA's experience in adopting NLP technology provides a clear illustration of both the advantages and challenges associated with SupTech for regulators and supervisors. It has enhanced supervisory, analytical and policy activities by extracting insights from large volumes of unstructured data. This

[19] See ESMA (2023b).

experience has also highlighted challenges related to document formats, algorithm design and human oversight.

In conclusion, SupTech offers immense potential for regulators and supervisors to improve the quality of financial regulation and oversight, reduce costs and enhance efficiency and effectiveness. As technology continues to advance, addressing challenges related to data access and quality, format, interpretability, skills and algorithmic transparency will be crucial to fully harness the benefits of SupTech.

References

Beerman K., Prenio J. and Zamil R. (2021). *SupTech tools for prudential supervision and their use during the pandemic*. BIS, FSI Insights on policy implementation No. 37. Available here.

BIS (2018) Bank for International Settlements. *Innovative technology in financial supervision (SupTech) – The experience of early users*. FSI Insights on policy implementation No. 9. Available here.

Crisanto J.C., Prenio J. and Singh M. (2022). *Emerging sound practices on supervisory capacity development*. BIS, FSI Insights on policy implementation No. 46. Available here.

Denis E. (2021). *The promises and pitfalls of SupTech for corporate governance-related enforcement*. Going Digital Toolkit Note, No. 10. Available here.

Di Castri S., Grasser M., Ongwae J., Mestanza J.M., Daramola D., Apostolides A., Christofi K., Rowan P., Wu T. and Zhang B. (2022). *The State of SupTech Report 2022.* University of Cambridge.

EC (2015) European Commission. *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 Single Market Strategy for Europe*. COM(2015) 192 final.

EC (2018) European Commission. *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 on a FinTech Action plan: For a more competitive and innovative European financial sector*. COM(2018) 109 final.

EC (2019) European Commission. *Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG): 30 Recommendations on Regulation, Innovation and Finance: Final Report to the European Commission.* Available here.

EC (2020) European Commission. *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.* COM(2020) 591 final.

EC (2021) European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Strategy on supervisory data in EU financial services.* COM(2021) 798 final.

EIOPA (2020) European Insurance and Occupational Pensions Authority. *Supervisory Technology Strategy.* Available here.

ESMA (2019a) European Securities and Markets Authority. *Final Report – Guidelines on Disclosure Requirements Applicable to Credit Ratings*. ESMA 33-9-320, 18 July 2019. Available here.

ESMA (2019b) European Securities and Markets Authority. *RegTech and SupTech – change for markets and authorities.* ESMA TRV Report, No. 1, 2019, pp.42-46. Available here.

ESMA (2021a) European Securities and Markets Authority. *RegTech/SupTech – potential for authorities*. ESMA TRV Report, No. 1, 2021, pp.55-57. Available here.

ESMA (2021b) European Securities and Markets Authority. *54,000 PRIIPs KIDs – How to read them (all).* ESMA TRV Report, No. 1, 2021, pp. 93-104. Available here.

ESMA (2022a) European Securities and Markets Authority. *Text mining ESG disclosures in rating agency press releases.* ESMA TRV Risk Analysis, 10 February 2022. Available here.

ESMA (2022b) European Securities and Markets Authority. *Parsing prospectuses: A text-mining approach*. ESMA TRV Risk Analysis, 29 November 2022. Available here.

ESMA (2023a) European Securities and Markets Authority. *ESMA Data Strategy 2023-2028.* Available here.

ESMA (2023b) European Securities and Markets Authority. *ESG names and claims in the EU fund industry.* ESMA TRV Risk Analysis, 2 October 2023. Available here.

FSB (2020) Financial Stability Board. *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions Market developments and financial stability implications.* Available here.

Lagarde C. (2018). *A Regulatory Approach to Fintech*. IMF Finance & Development, June 2018. Available here.

OECD (2021) Organisation for Economic Co-operation and Development. *OECD Business and Finance Outlook 2021: AI in Business and Finance,* OECD Publishing, Paris. Available here.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

World Bank (2018). *From spreadsheets to SupTech: Technology solutions for market conduct supervision*. Available here.

4. RegTech[1]

Maha Abbassi
Policy Expert at European Banking Authority

1. RegTech: definition and growth trajectory

RegTech is defined as "any range of applications of technology-enabled innovation for regulatory compliance and reporting requirements implemented by a regulated institution, with or without the assistance of a RegTech provider."[2] It differs from SupTech, which is the use of technology-enabled innovation by supervisors or for supervisory purposes.

The term 'RegTech' seems to have been used for the first time around 2015. However, the technology and its applications can be retraced back to before that, and it gained more attention after the financial crisis when financial institutions started tackling additional regulatory requirements. The need to leverage technological solutions has also been exacerbated as supervisors have become increasingly data-driven.

The most widespread areas of RegTech applications are anti-money laundering and countering the financing of terrorism (AML/CFT) [including know-your-customer (KYC), and transaction monitoring], fraud monitoring and prevention, regulatory reporting, information and communication technology (ICT), identity management, cybersecurity, and environmental, social and governance (ESG)-related fields.

[1] This chapter is based on presentations and discussions during the EU-SDFA RegTech workshop organised by the EBA and on publicly available information. The views expressed here are those of the author and do not necessarily reflect those of the EBA.

[2] As defined in EBA (2021).

RegTech enhances compliance in these areas using various techniques and technologies, such as machine learning (ML) and artificial intelligence (AI), robotic process automation (RPA), big data and analytics, blockchain and cryptography. Cloudification and new-generation data and software architectures are also considered among these techniques. There are, however, many other emerging technologies and techniques.

There are two main categories of added value of these applications: (i) modernisation, automation and streamlining of business processes that lead to efficiency and cost reduction, including through reducing error rates, achieving the same results with better tools and at a lower cost; and (ii) enhancing risk management with new insights, and in this case the results are augmented using technology and potentially enhanced customer experience as a result of prior optimisations.

It is to be noted that the needs and interests of institutions and the risks they are exposed to can differ depending on their characteristics, for example between a large global systemically important institution or a small local financial institution.

RegTech companies have a growth curve parallel to that of fintechs generally but with some lag. According to market studies, the global revenue of RegTech providers was 7 billion euros in 2021 and it is projected to increase to 20 billion euros by 2027.[3] Global investment in RegTechs grew from 3.4 billion euros in 2017 to 10.7 billion euros in 2022.

Despite a slowdown in 2022, the adoption of RegTech is increasing overall,[4] and there is an increasing appetite for RegTech solutions among the financial industry. In terms of geographical distribution, the European region hosts close to 40% of RegTech providers, right behind North America, which is home to over 45%.

2. Examples of RegTech applications

RegTech solutions cover a variety of fields, some of which are presented below.[5] At the EU level, in 2021, the EBA published a RegTech[6] report describing the RegTech landscape in the EU. It tackled on several of the applications (mentioned here) in greater detail.

[3] See KPMG (2023).

[4] See Thomson Reuters (2023).

[5] Based on EBA (2021) and Deloitte RegTech landscape available here.

[6] See EBA (2021).

Requirements[7] that the considered RegTech solutions help to meet include the Anti-Money Laundering Directive[8] (AMLD), with a particular focus on the customer due diligence (CDD) requirements. For instance, according to this Directive, financial and other (obliged) entities need to ascertain the identity of their customers and verify it using reliable and independent sources or they need to identify the customer's beneficial owner. Additionally, such obliged entities must evaluate and gather information on the purpose and intended nature of the business relationship and monitor it continually, including transaction monitoring and updating the underlying information.

The requirements mentioned also include various reporting requirements mandated by the Capital Requirements Regulation[9] (CRR) and the Mortgage Credit Directive[10] (MCD), which specify, among other things, an obligation to assess the borrower's creditworthiness. Furthermore, the applications refer to several guidelines, such as EBA guidelines on loan origination and monitoring,[11] EBA guidelines on the use of remote customer onboarding solutions[12] and EBA guidelines on ICT and security risk management.[13]

2.1 Regulatory reporting

RegTech solutions help to enhance regulatory reporting by streamlining it and combining it with analytical capabilities. There are multiple aspects of these efforts. In the past, reporting used to be a file-based process, often requiring manual interventions. While the process is still mainly file-based, the first step to reduce costs is automatically generating and validating these files. It is advantageous to separate the software that builds the expected report format and runs validation rules from the core systems that generate the data used in the reporting. In this way, the core data can serve multiple purposes, such as risk management and other internal matters. Checking the data once for all purposes can help focus staff efforts on economic objectives. Furthermore, managing reports separately can provide flexibility in reporting formats and calendars.

[7] For a complete overview, refer to EBA (2021).

[8] See Directive (EU) 2015/849.

[9] See Regulation (EU) No 575/2013.

[10] See Directive 2014/17/EU.

[11] See EBA (2020).

[12] See EBA (2022).

[13] See EBA (2019).

RegTech reporting solutions also map the source data to a data model that can later be used to generate various required reports. Additionally, these solutions can include data aggregation features. They are often augmented with analytical capabilities, including integrated visualisation tools, which can be useful for internal risk management purposes.

2.2 Anti-money laundering applications

Many RegTech solutions exist to help address the obligations of credit and financial institutions regarding identification and verification processes [commonly referred to as know-your-customer (KYC)]. Specifically, the rise of online banking, notably during the Covid-19 pandemic, has increased the need for reliable, compliant and swift procedures for remote onboarding of customers. Regarding verification, these solutions are mainly provided through third parties that obtain information from open-source intelligence (OSINT), or their partners such as electricity companies and postal services, to verify addresses. In addition, automatic image processing, optical character reading (OCR) and machine learning are some of the technologies used to recognise facial patterns and compare them to the identity documents provided. Other techniques include biometrics and geographical localisation data. In addition, machine learning algorithms detect fraud by leveraging various collected data sets. Finally, these techniques are also used for initial and continual customer risk assessment, including screening for politically exposed persons (PEPs).

Another use in the area of AML/CFT is transaction monitoring, as credit and financial institutions have to assess the risk of their customers and the ML/TF risk associated with their activities. Transaction monitoring is historically rule-based. However, it leads to a large number of false positives. RegTech solutions can help provide alternative methods to identify suspicious transactions which are model-based, using AI/ML, for instance. They also offer automated solutions for sanctions’ screening and watchlist filtering. In particular, machine learning techniques combined with graph or network analysis can yield results with lower false positive rates, thus reducing the workload for compliance analysts.

2.3 Creditworthiness assessment

In some cases, it is now possible for loans to be granted in a few minutes thanks to automatic creditworthiness assessments. These assessments rely on RegTech solutions that harness the power of machine learning, artificial intelligence, cloud computing and real-time analytics. The revised Payment Services Directive[14] (PSD2) made it easier for credit institutions to access transaction data, which is used alongside publicly available data to model consumer habits. It is to be noted that financial institutions that provided feedback for EBA RegTech report stated that they do not use social media information for these assessments due to reputational risks.

2.4 Compliance matters related to crypto-assets

With the advent of blockchain, solutions that specialise in supporting financial institutions and cryptocurrency businesses in their compliance with regulatory requirements are becoming more available. They offer various services, including on-chain transaction monitoring, KYC, fraud detection and prevention, risk assessment of analysed entities and sanctions' monitoring. Some of these solutions also provide government agencies with investigation and forensics tools. The technologies used include blockchain analytics, artificial intelligence and machine learning.

2.5 Other examples

There are several other types of solutions, for instance ICT risk and cyber-security management solutions, sustainability disclosures, regulatory watch, compliance-as-a-service solutions for the management of compliance documents and processes, privacy management [related to the General Data Protection Regulation (GDPR)] solutions, legal text search engines, regulatory co-pilots and adverse media scanning tools.

3. Associated risks

From the perspective of supervisors, it is important to recognise the benefits of RegTech solutions while also being diligent in identifying potential risks. For instance, reporting solutions may be used by financial institutions (FIs) to

[14] See Directive (EU) 2015/2366.

avoid taking responsibility for ensuring high-quality data is reported to authorities, which would go against BCBS 239 principles.[15] Therefore, RegTech providers should be fully transparent about the controls they implement so that FIs can explain them to supervisors.

A concentration of risk on the side of solution providers is another concern. If only a few major players emerge, many financial entities can become susceptible to the same operational risks. In addition, business continuity risks need to be adequately managed. Legal and reputational risks can arise from fraudulent activities or processing of illegal funds due to non-compliant AML/CFT solutions.

New technologies may also introduce additional ICT risks such as unauthorised access to data through cloud-based analytical systems. It is crucial to have robust safety measures in place to protect against cyber threats. Another concern is possible consequences of outdated software and data.

Furthermore, if RegTech solutions fail to comply with data protection and privacy regulations, it could lead to legal and reputational risks for FIs. Data breaches or a lack of consumer consent could cause harm to consumers. More clarity may be needed regarding the data protection controls of RegTech providers, including data storage locations and monitoring responsibilities.

4. Challenges in RegTech development

Despite the interest in the value proposition and the diversity of use cases, several barriers to RegTech development have been identified by both RegTech vendors and financial institutions.

4.1 Barriers to business development from the perspective of RegTech providers

Compared to fintechs, RegTech have limited access to funding, venture capital and joint ventures.

Difficulty with sales could arise from compliance being a sensitive domain for financial institutions. RegTech startups are expected to provide perfect products from the start as their clients are expected to be fully compliant. Financial institutions would not be satisfied with a minimal viable product (MVP) that only partially addresses a given compliance matter, just as a super-

[15] See BCBS (2013) and ECB (2023) European Central Bank. *Guide for effective risk data aggregation and risk reporting.* (Public consultation draft). Available here.

visor would not be satisfied with partial compliance of a financial institution. In comparison, an MVP can focus on one feature and augment the solution incrementally for other types of fintech products unrelated to regulatory requirements. However, this concern only applies if the RegTech solution aims to completely replace a given compliance software in the financial institution. Using these RegTech solutions as complements rather than complete replacements for existing systems is always possible.

In addition, several factors can erode the potential for profit and subsequently limit access to funding. Staff require specialised skills, resulting in higher costs, particularly for marketing and sales staff. In addition, sales cycles and procurement processes are very long, which leads to higher customer acquisition cost. At the product level, differences between national regulations make it challenging to scale and expand the client base.

RegTech providers also highlighted that financial institutions tend to perceive the RegTech sector as immature and lack awareness of available solutions operating in other jurisdictions.

4.2 Implementation challenges

There are barriers to implementation which vendors and financial institutions see as particularly challenging. The obstacles to integrating RegTech solutions in clients' legacy applications are mainly linked to a lack of capabilities in application programming interfaces (APIs) on the clients' side.

In addition, clarifying security, data privacy and protection issues and possible legal and regulatory obstacles to adopting those solutions may take substantial time and effort. In this context, RegTech providers perceive requirements for processing personal data to be of significant relevance, followed by the evolving AML/CFT regulatory requirements and requirements for outsourcing. Moreover, substitutability between different RegTech solutions offering the same service can be challenging. At the same time, financial institutions could require it to handle third-party and business continuity risks.

5. How to overcome the challenges

5.1 Leveraging EU initiatives and frameworks

The EU is actively prioritising digital matters. It is committed to being fit for the digital age by facilitating and fostering innovation and competition, while at the same time achieving the regulatory objectives of financial stability, market integrity and consumer protection, and maintaining technological neutrality. Regulators and supervisors are engaging in various efforts to contribute to these objectives and to become tech-ready and data-driven. In the RegTech field, several components of the EU Digital Strategy,[16] including EU digital finance[17] and EU data strategies, can be leveraged. In the field of reporting and data in the context of the EU supervisory data strategy, the European Commission, the ESAs and the national competent authorities are working towards modernising and integrating EU supervisory reporting while minimising the reporting burden for all relevant parties.

These efforts fall in two different categories. On the one hand, an integrated approach to reporting is being developed to remove redundancies and harmonise reporting for financial entities. Examples include i) the DMP ReFit[18] by EBA and EIOPA, which evolves the DPM standard to support more complex data, larger volumes and better scalability; ii) the Integrated Reporting Framework (IReF),[19] which aims to integrate the Eurosystem's statistical requirements for banks in a single standardised reporting framework applicable across the euro area; and iii) the BIRD project,[20] in which several EU institutions and national central banks collaborate with the private sector in a joint effort to define a data dictionary and model across the various reporting requirements (statistical, prudential and resolution).

On the other hand, new experiments with modern techniques are being explored to change the approach to reporting requirements altogether. An example is the MRER[21] (machine-readable and executable representation of reporting requirements) project, which was launched by the European Commission and executed in close cooperation with ESMA to study whether such representation can enhance the efficiency and effectiveness of reporting development and to identify any legal barriers to such approaches.

To facilitate RegTech adoption, ESAs and national authorities are engaging in activities supporting these new solutions. For example, they provide guidance and maintain dialogue with the private sector using various formats to help

[16] See EC European Commission webpage, A Europe fit for the digital age

[17] See EC European Commission webpage, Digital Finance Package

[18] See DPM 2.0 Press release

[19] See IReF webpage

[20] See BIRD webpage

[21] See Commission workshop on MRER

navigate regulatory matters, they are reachable through innovation hubs, and the established regulatory sandboxes allow some ideas to be tested in practice.

5.2 Considering new approaches

At the level of financial institutions, there are several elements to consider when facing the abovementioned challenges. First, when the effort seems colossal and the changes too complicated, it is good to revert to basics, taking an incremental approach and focusing on things that can be controlled. This could mean that financial institutions re-assess where RegTech is most needed. Areas and/or processes currently with the highest costs, most complex procedures and lowest added value could be great places to start. It is also helpful to identify which requirements are the most difficult to address and to clearly understand the pain points and their root causes in order to determine whether technological solutions can address them. In some areas, a purely technological approach can be of limited benefit due to overly complex procedures, organisational problems and data quality issues.

Second, in preparing make-or-buy decisions, it seems that from the perspective of financial institutions the main determinant for a make-or-buy decision is still the associated cost. There are also other factors, such as the desire to keep a specific competence internal and whether these solutions are easily substitutable if any issues emerge. In addition, from the RegTech providers point of view, financial institutions should focus on their ability to clearly formulate and communicate to RegTech providers an exact idea of the solutions they seek. Furthermore, integration issues have to be assessed too. Many financial institutions are exposed to significant legacy systems issues, where for better adoption of RegTech and to realise the associated benefits, the financial institution should consider whether it is better to upgrade the systems or if it is possible to integrate with RegTech without doing so. Finally, in the implementation phase, a major area to consider is change management and third-party management, where relevant.

At the industry level, RegTech providers indicated that they perceive benefits from more joint ventures with financial institutions and sandbox environments run by financial institutions, which could facilitate raising the awareness of institutions of the available RegTech solutions before engaging in a procurement process. In addition, various industry actors have expressed a need for deeper horizontal collaboration between regulators and supervisors covering the various regulatory areas that a single entity needs to comply with, such as in the fields of data-sharing and data collaboration to fight financial crime and to enhance customer onboarding procedures.

Finally, it is crucial for all the parties involved, including regulators, to invest in skills to keep up with technology changes and associated risks.

6. Conclusion

As the regulatory context continues to evolve and as efforts towards harmonisation and standardisation continue, there are new opportunities for RegTech to grow further. Various surveys[22] show industry optimism in this regard. As an example of new applications for RegTech that might emerge, some industry actors[23] suggest that this can be related to AI governance. It is also possible that specific RegTech offers will evolve to service crypto-asset service providers and issuers. In addition, with the regulation on digital and operational resilience[24] (DORA), existing cyber risk-related solutions could develop further to support compliance with DORA requirements.

To conclude, it can only benefit regulators and supervisors to prioritise even further technology-readiness and technology-fluency, as this would also help render supervision and policymaking smoother and faster. In addition, new forms of holistic cooperation between authorities in innovation hubs and regulatory sandboxes may become necessary in the future for supervisors and regulators to consistently keep up with changes in the financial industry.

[22] E.g. see Thomson Reuters (2023).

[23] E.g. IBM article on AI governance

[24] Regulation (EU) 2022/2554.

References

BCBS (2013). *Principles for effective risk data aggregation and risk reporting*. Available here.

Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010.

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 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.

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.

EBA (2019) European Banking Authority. *EBA Guidelines on ICT and security risk management*. EBA/GL/2019/04. Available here.

EBA (2020) European Banking Authority. *Guidelines on loan origination and monitoring*. EBA/GL/2020/06. Available here.

EBA (2021) European Banking Authority. *EBA analysis of RegTech in the EU financial sector*. EBA/REP/2021/17. Available here.

EBA (2022) European Banking Authority. *Guidelines on the use of Remote Customer Onboarding Solutions*. EBA/GL/2022/15. Available here.

KPMG (2023). *Unlocking the potential of RegTech*. Available here.

Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

Thomson Reuters (2023). *Fintech, RegTech, and the role of compliance in 2023.* Available here.

5. Analysing digital business models[1]

Adrian Mora-Moreno
Expert on digital finance at European Insurance and Occupational Pensions Authority

The evolution of technology and the integration of it in business processes have a profound impact on every stage in the value chain in the financial sector. This transformation is exemplified by the emergence of startups, which often engage in collaborative agreements with established enterprises, technology firms, BigTech companies and IT platform providers entering the financial market. In addition, digitalisation creates new distribution channels such as online platforms and introduces innovative ways to engage with customers, offering significant potential benefits. Moreover, this digital revolution introduces new types of competitors and potential disruptors of traditional business models, including mixed activity groups (MAGs) offering financial and other services.

The impact of digitalisation on market competitiveness and the dynamics of distribution is expected to continue to grow. To effectively navigate these evolving dynamics, it is crucial for regulators and supervisors to profoundly understand the impact of digitalisation in business models and the associated risks and sustainability over the long term. Supervision of these changing business models is paramount to ensure the stability and integrity of the financial ecosystem.

This chapter starts by introducing the concept of business models, putting

[1] The content of this chapter reflects the opinions of the author and do not necessarily reflect the views of EIOPA.

particular emphasis on the increasing influence of digitalisation on business models in the financial sector. Following this, it conducts an analysis of the pivotal role that the supervision of business models, particularly in the context of the evolving digital landscape, plays in assisting supervisors in meeting their responsibilities. Finally, it presents the work undertaken by the European Supervisory Authorities (ESAs) in this field to support the efforts of national competent authorities (NCAs).

1. The increasing role of business model digitalisation

A business model is the means by which an entity generates value from its business. All business models share common characteristics but each one has its own specific characteristics.[2] From a pragmatic perspective, a business model plays a pivotal role in shaping various factors, including but not only the fundamental products and/or services offered, the marketing, distribution and sales strategies, the operational procedures and protocols, and interconnected structural, collaborative and financial agreements with other entities involved in the value chain, such as outsourcing and engagement with third-party entities.

Moreover, business models are dynamic and evolve over time. Business model innovation is the art of enhancing advantage and value creation by making simultaneous – and mutually supportive – changes to both an organisation's value proposition to its customers and its underlying operating model.[3]

In the context of the financial service industry, business model innovation has paramount importance in response to the transformative effects of digitalisation. This transformation has diverse dimensions. There is growing consumer demand for streamlined access to products and services from a single point of entry using smartphones or computers 24/7 from any location. Furthermore, the use of emerging datasets, including ones from the internet of things (IoT), combined with technological advances offers a way to establish more efficient, prompt and automated procedures.

Digitalisation by financial sector entities involves exploring, analysing and integrating technological innovations such as platforms, applications, chatbots, cloud services, data analytics, artificial intelligence and more. These technologies are harnessed to craft, deliver and capture value. This transform-

[2] Fielt (2013).

[3] Boston Consulting Group. *Business model innovation.* Available here.

ative process often involves leveraging the internet and other digital tools, including cloud services and digital platforms, to not only offer customers new products and services but also to streamline various aspects of the business such as marketing and sales, claims processing and customer service. In the course of this adaptation, supplementary elements enrich the value chain. These involve tailoring products to cater to specific customer needs, devising personalised pricing models, ensuring round-the-clock accessibility through distribution channels and providing ongoing support. The infusion of added value also extends to back-end business processes, improving stakeholder interaction, fostering customer loyalty, and catalysing new opportunities through innovations in product offerings at the front end.

In the light of these dynamics, all stakeholders in the market have adopted digital strategies to varying extents. Traditional financial entities from the securities, banking and insurance sector have embraced digitalisation to create innovative business models that cater to changing consumer preferences and technological advances. Simultaneously, entities born in the digitalisation era, such as insurtech startups, neobanks and larger technology corporations, i.e. BigTechs, are making inroads into financial markets with innovative propositions. Growing interactions have been observed between incumbent financial institutions, fintechs and BigTechs in a variety of co-operation models, e.g. partnerships, joint ventures, outsourcing and sub-outsourcing, mergers and acquisitions. These firms are also partnering to co-innovate and provide new products or services leveraging their complementary competencies.[4]

In conclusion, the ongoing process of digitalisation is profoundly reshaping the landscape of financial entities, compelling them to adapt and evolve their business models. Within this transformation, various entities in the financial market are employing diverse approaches and varying levels of innovation. For instance, traditional financial firms may choose to integrate robotic process automation to enhance their operational efficiency and employ chatbots and digital platforms for customer communication. In contrast, emerging players like insurtech startups and similar entities may opt for entirely digital business models offering innovative services through digital platforms.

[4] JC ESAs (2022).

2. Business Model Analysis (BMA): Evaluating strategies of supervised entities in the digital context

As the growing digitalisation of business models continues to reshape the financial services sector, the importance of effective supervision becomes ever more relevant. The objective of conducting BMA is to provide supervisors with a comprehensive understanding of various key elements.

BMA encompasses an evaluation of the viability and sustainability of an entity's existing and prospective business model. This evaluation takes into account various critical factors, including the organisation's strategic approach, risk tolerance, customers, the value proposition it offers, the intricacies of the value chain and the underlying profit generation mechanism that forms the core of the business model. Furthermore, this analysis serves the purpose of identifying and assessing potential risks inherent in the business model.

In the light of these objectives, the aims of the BMA can be grouped in three key areas: (a) to establish an understanding of the existing business model and its sustainability by discerning the mechanisms of value creation ('who-what-how-why'); (b) to anticipate potential transformations in the model due to strategic decisions made by the entity; and (c) to evaluate the consequences of alterations in the business environment – both internal and external. This holistic assessment contributes to a forward-looking evaluation of the durability of the business model.

BMA is of paramount importance in the three sectors, serving as a pivotal tool for regulators and supervisors to effectively execute their responsibilities. In the context of prudential supervision in the banking, insurance and investment sector, BMA plays an integral role in supervisory review and evaluation process (SREP) methodology.[5] The BMA should encompass assessment of the capacity of the supervised entity to generate profits, taking into account both immediate and prospective business sustainability, and prevalent and forthcoming key risks and vulnerabilities. It is applicable to various corporate entities and organisational tiers, such as group-wide assessments, individual entities, intermediaries, specific business lines and ancillary service providers. As a constituent of forward-looking supervision, BMA serves as a conduit for supervisors to delve into the strategies of entities to generate profit, their current and future risk exposure, and the array of threats and opportunities they encoun-

[5] Art. 97, Directive 2013/36/EU; art. 36, Directive (EU) 2019/2034; art. 36, Directive 2009/138/EC.

ter. It aids early identification and mitigation of foundational issues. The establishment of sustainable business models, ensuring viable profitability across extended timeframes, forms a cornerstone of a robust financial market. BMA serves as a supervisory tool utilised both during the licensing procedure and in ongoing supervision. This may include comparative BMA exercises for certain entities, often initiated by early warning indicators for specific companies or prior to the launch of new products.

In the process of conducting a BMA, regulatory authorities have the capacity to identify nascent strategies that could potentially yield risks or uncertainties down the line. Among the array of risks, uncertainties may emerge in the digital context, either due to novel risks associated with the digitalisation of business models or due to the adoption of a strategy that disregards emerging technologies and the imperative of digitalisation. While this might not raise immediate concerns, neglecting it could potentially evolve into a sustainability challenge to the business model in the future.

Given the aforementioned points, it is imperative that management bodies of supervised entities immerse themselves deeply in comprehending the ramifications of their business models, along with the associated prudential and conduct risks involved. Specific conduct and prudential risks are typically inherent in any given business model and/or business strategy and its execution. Entities must proactively recognise these risks, institute efficient measures to mitigate and manage them, establish appropriate checks and balances, and consistently reevaluate them in tandem with shifts in the business model or external circumstances. In extreme cases, entities might opt to abstain from engaging in the specific activity or practice giving rise to substantial risk.

Fragmentation of the value chain, the rise of digital platforms, the presence of BigTechs, MAGs, fintechs and the emergence of new forms of cooperation have collectively accelerated the evolution of financial services and business models through digitalisation and innovative technologies. In the rapidly changing landscape of financial services driven by digitalisation and innovative technologies, conducting assessments of business models offers financial supervisors a valuable opportunity to gain deeper understanding of the factors that generate both opportunities and vulnerabilities within the entities they oversee and enables them to craft more tailored and appropriate supervisory strategies that are well-aligned with the realities of changing business models.

3. The role of ESAs in supporting the supervision of digital business models

European Supervisory Authorities (ESAs) supervise digital business models aiming to ensure that the financial sector is safe and sound in the digital age. ESAs actively take multiple measures to assist the NCAs and contribute to the supervision of digital business models in the EU financial sector. These steps include the following.

- Offering guidance and recommendations to NCAs and the European Commission. In January 2022 in response to a call for advice on digital finance from the European Commission, the ESAs released a report. This report presents insights into the changes that the application of innovative technologies is bringing to the structure of the EU financial sector. The ESAs recommend a series of actions to the European Commission to strengthen the regulation of EU financial services and enhance supervisory capabilities in line with these developments. The recommendations are intended to address the evolving landscape of digital finance and ensure sustained relevance and effectiveness of the EU's financial regulatory and supervisory framework.[6]

- Monitoring trends and developments and enhancing cooperation. The ESAs, both individually and jointly through the Joint Committee (JC), monitor trends and developments in the digital financial sector. This includes monitoring the emergence of new digital business models, the use of new technologies and the risks posed by these developments.[7] In addition, the European Forum for Innovation Facilitators (EFIF) within the JC provides a platform for supervisors to meet regularly to share experiences from engagement with firms to innovation facilitation (regulatory sandboxes and innovation hubs) to share technological expertise and to reach common views on the regulatory treatment of innovative products, services and business models, overall boosting bilateral and multilateral coordination.[8]

- Engaging with stakeholders. The ESAs engage with stakeholders, such

[6] JC ESAs (2022).

[7] JC ESAs (2016).

[8] European Forum for Innovation Facilitators. See here.

as financial institutions, technology companies and consumer groups, to discuss the supervision of digital business models. This engagement helps the ESAs understand the challenges and opportunities posed by digitalisation and to develop effective supervisory approaches.

The ESAs' work on supervising digital business models is ongoing. They will continue to monitor trends and developments, engage with stakeholders and enhance cooperation to ensure that the financial sector is safe and sound in the digital age. In addition to the abovementioned joint work, each of the ESAs has done work related to emerging business models, including the following.

In 2021, the European Banking Authority published a report on the use of digital platforms in the financial sector.[9] The report argues that one aspect of structural change is an increasing reliance on digital platforms. It presents different types of platforms, such as comparators, financial institutions, ecosystems and enablers and discusses the risks associated with platformisation, such as ICT and operational resilience risks, concentration and interconnectedness risks, customer data risks, reputational risks, competition and level playing field risks and new forms of ML/TF risks. The report also makes recommendations, which are based on seven topics: supervisory oversight of third-party service providers; clarity in classifying the cross-border provision of digital services; consumer protection and conduct issues; skills and resources of NCAs to effectively monitor coverage of MAGs by sectoral prudential consolidation rules; systemic interconnectedness; risks posed by MAGs/BigTech providing financial services; and a structured cooperation framework connecting relevant authorities. This work informed the ESAs' abovementioned response to the EC on digital finance.

In 2023 the European Securities and Markets Authority published a supervisory briefing on supervisory expectations in relation to firms offering copy trading services.[10] Copy trading is a service that involves trading client's assets based on the trades of another trader. The briefing outlines expectations of how MiFID requirements should apply to copy trading business models.

Digital business model analysis is among the priority areas outlined in a supervisory convergence plan for 2023 issued by the European Insurance and Occupational Pensions Authority.[11] In the plan, EIOPA emphasises the importance of supervisors reflecting on ongoing changes to gain better understand-

[9] EBA (2021).

[10] ESMA (2023).

[11] EIOPA (2023).

ing of new technology-driven business models and strategies, assess the associated risks and determines their long-term sustainability. In alignment with the commitments outlined in the plan, EIOPA is actively developing supervisory convergence tools to assist NCAs in conducting business model analyses in the context of the digital insurance market.

4. Conclusion

The impact of technology in the financial sector is profound. It is reshaping the entire value chain and driving dynamic changes. The continual evolution of business models in response to these shifts presents both opportunities and risks, underscoring the importance of effective supervision. BMA assists supervisors in comprehending critical elements and supports forward-looking oversight. The ESAs are actively taking measures to assist the NCAs and contribute to the supervision of digital business models in the EU financial sector.

References

Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).

Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU.

EBA (2021) European Banking Authority. *Report on the use of digital platforms in the EU banking and payments sector*. EBA/REP/2021/26. Available here.

EC (2020) European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions on a Digital Finance Strategy for the EU*. COM(2020) 591 final.

EC (2021) European Commission. *Request to EBA, EIOPA and ESMA for technical advice on digital finance and related issues*, Ref. Ares(2021)898555, 02 February 2021.

EIOPA (2023) European Insurance and Occupational Pensions Authority. *Supervisory Convergence Plan for 2023*. EIOPA-BoS-23/039, 1 February 2023. Available here.

ESMA (2023) European Securities and Markets Authority. *Supervisory Briefing: On supervisory expectations in relation to firms offering copy trading services*. ESMA35-42-1428, 30 March 2023. Available here.

Fielt E. (2013). *Conceptualising Business Models: Definitions, Frameworks and Classifications*. Journal of Business Models. Vol.1, No. 1, pp. 85-105. Available here.

JC ESAs (2016) Joint Committee of the European Supervisory Authorities. *Towards supervisory convergence, the Joint Committee of the European Supervisory Authorities*. Luxembourg: Publications Office of the European Union, 2016. Available here.

JC ESAs (2022) Joint Committee of the European Supervisory Authorities. *Response to the European Commission's February 2021 Call for Advice on digital finance and related issues: regulation and supervision of more fragmented or non-integrated value chains, platforms and bundling of various financial services, and risks of groups combining different activities*. ESA 2022 01, 31 January 2022. Available here.

6. Selected case studies[1]

Maha Abbassi
Policy Expert at European Banking Authority

Giulio Bagattini
Risk Analysis Officer at European Securities and Markets Authority

Andres Lehtmets
Seconded National Expert on InsurTech at European Insurance and Occupational Pensions Authority

1. Introduction

In the context of the EU-SDFA, the ESAs have organised targeted workshops to discuss practical issues related to the interaction between digital finance and the existing regulatory framework, and practical matters relevant to supervisors.

This chapter presents three selected use cases from ESMA's workshop on SupTech, EIOPA's workshop on Digital Business Model Analysis and the EBA's workshop on RegTech.

As part of its efforts to increasingly leverage the potential of SupTech, ESMA has developed automated methods to analyse the prospectuses of financial securities. This project showcases how text-processing tools can transform unstructured information from documents into structured data for quantitative analysis.

EIOPA has investigated the risks and benefits of open insurance develop-

[1] The views expressed here are those of the authors and do not necessarily reflect those of the European Supervisory Authorities.

ments and new applications. The selected use case of an insurance dashboard that displays a consumer's insurance policies, along with a comparison tool of coverages and prices from different providers, helped stir the discussion on such technical and supervisory implications of setups.

The EBA's example and the ensuing discussion elaborated on the benefits and challenges in data sharing and collaborative analytics in the fight against money laundering and terrorist financing.

2. NLP applied to prospectuses

The prospectuses of securities issued in the EU under the Prospectus Regulation can be lengthy – sometimes spanning up to 1,000 pages – and filled with technical language. Therefore, they serve as an ideal ground to develop SupTech. In particular, natural language processing (NLP) techniques provide novel tools for supervisors and policymakers to facilitate their assessment of the application of the Prospectus Regulation by issuers and to identify themes which potentially warrant closer monitoring.

Against this background, the project[2] explored a number of linguistic features of prospectuses, such as their length, the 'effective' length once all documents referenced by links are included, the extent to which duplication of text occurs, and the complexity of the language used. It also examined the contents of specific sections and required phrases, such as the risk factors section.

Approximately 593,000 pages of text from 3,220 documents were analysed using computer code that counted the number of pages of each document and recognised their language.

The next step involved extracting all hyperlinks from the PDF documents. The use of hyperlinks is relevant because it yields an alternative measure of the amount of information that an issuer makes available in compliance documents. In addition, a large number of sources that are external to the prospectus may make it more difficult for investors and supervisors to retrieve all the content relevant to their understanding of the product. Once the hyperlinks were identified, their functionality was verified by accessing the linked webpages via automated connections. Then, the documents linked to in each prospectus were downloaded, which resulted in c. 950,000 pages of text – or almost 300 additional pages per prospectus. These extra texts include additional marketing material, information on the issuer, periodic reports and financial accounts.

[2] Some of the findings in this project are described in ESMA (2022a).

The project then turned to analysing the risk factors laid out in the prospectuses, i.e. disclosures made by issuers regarding how risks affect the financial instrument. The information disclosed and how it is presented have significant implications for policy, supervisory convergence and risk assessment, but a systematic analysis of this information by a human supervisor is difficult given the lengthy text typically used and the unstructured format of the disclosure. The risk factor section of each prospectus was identified using a rules-based algorithm constructed to recognise the internal structure of the document, and further segmented into distinct risk factors. The results of this exercise showed that prospectuses of structured finance products like derivatives and asset-backed securities tend to have more risk factors than more straightforward products like shares and debt instruments. At the same time, the number of risks presented in prospectuses for the same type of instrument varies widely, ranging from just a few to a hundred. This raises questions about the different approaches adopted by issuers. The risk factors were then assigned to specific topics based on keywords, such as interest rate risk, for further investigation. The language used by different issuers for each topic was compared in order to understand if the risks disclosed were tailored to company-specific sources of risks and the unique characteristics of their financial instruments. This linguistic analysis highlighted a number of cases of identical or highly similar language used by multiple issuers when describing certain risks. This observation suggests that there may be industry-standard risk descriptions or templates that issuers employ. By uncovering these insights, the project provided examples of actionable practices for regulators and supervisors to enhance their understanding of risk disclosures in prospectuses, prioritise supervisory actions and help them make informed decisions in their oversight roles.

Next, some tools to analyse the linguistic complexity and diversity of prospectuses were examined. First, several ways to assess the complexity of a text were assessed, which ranged from basic metrics such as sentence length to more complicated econometric-based methods. The proposed analysis employed a linguistic measure called Yule's I, which measures the uniformity of vocabulary in a text. Somewhat surprisingly, prospectuses describing instruments with more complex payoffs and features, such as asset-backed securities and derivatives, tend to have less diverse (i.e. more uniform) vocabulary. In contrast, typically more straightforward instruments like equities and debt instruments tend to have a greater variety of language. A possible reason for this pattern is that issuers of complex instruments use simpler language to compensate for the inherent complexity of the information presented in the prospectus to make the instrument more palatable to investors – a pattern that, if confirmed, would have relevant implications for policymakers to assess.

Finally, the project offered insights into methods to assess repetition and duplication of text in a document. The extent to which duplication of text occurs in compliance documents is of particular relevance from an investor protection perspective, insofar as repetition of language can lead to reader fatigue and the risk of key provisions being overlooked. Different methods were considered to isolate distinct sentences in the raw text and compute the extent to which identical sentences appear more than once in each document. It was shown that longer documents do not always include correspondingly greater amounts of information. The rate of repetition of text also tends to be higher in financial security prospectuses than in a sample of comparable investment fund prospectuses.

Overall, analysis of prospectuses using NLP provides policy-relevant insights into the accessibility of these documents for investors and suggests that prospectuses may not always convey key information optimally. The project illustrates the usefulness of text mining as a SupTech tool. The development of algorithms capable of analysing the content of prospectuses opens new possibilities for supporting supervisory assessments, as key information which would be time-intensive for the human eye to find can be extracted in seconds from lengthy documents. Such information can also be used for supervisory convergence activities, for example in peer reviews.[3] This facilitates the detection of anomalies, which supervisors may subsequently prioritise for manual inspection. The methodologies developed can assist the ability of supervisors to systematically monitor risks faced by investors in relation to specific financial instruments and how clearly and thoroughly these risks are presented in the prospectus.

NLP-based analyses also have limitations. For instance, the choice of linguistic metrics used as criteria in the text analysis is subject to prior selection and judgement. The advantages and pitfalls of rules-based vs. machine-learning-based approaches in analysing heterogeneous documents such as prospectuses using NLP were also taken into account. While machine-learning-based NLP tools were partly used, in many cases it was evaluated that a rules-based approach would yield the best results given the characteristics of the corpus of documents. Although solutions and methodologies were tailored to achieve specific objectives, this project provided concrete tools and ideas that can inspire a similar NLP analysis in the work of supervisors.

[3] For example, see ESMA (2022b).

3. Open insurance

A discussion on open finance has been taking place for some time, focusing so far mainly on the banking sector (open banking). Internal application programming interfaces (APIs) in insurance have been in place for a while, but the focus has only recently shifted towards opening up APIs to the outside world to offer better services to policyholders or achieve greater market competition. However, in the absence of any regulatory or self-regulatory requirements, developing such services entails bilateral agreements and the bridging of different standards to ensure interoperability. Open insurance would involve some standardisation or possible compulsory data-sharing initiated and consented to by the customer.

A recent European Commission proposal for a framework for Financial Data Access[4] (FIDA) aims to expand open finance into other sectors, including the insurance and pensions sector, by creating a possibility but no obligation for customers to share their data with data users in secure machine-readable format. These developments have increased the need to better understand open insurance and the related risks and benefits from the supervisory perspective. There are still many questions on how certain new open insurance services would look and should be treated, what existing regulation should be applied and how the new proposed regulation might impact the sector and its supervision.

Consequently, one of the case studies explored during the workshop at EIOPA on Digital Business Model Analysis focused on a concrete, specific and detailed open insurance case to facilitate better understanding of implications among the supervisory community and to explore technical issues and supervisory challenges in a concrete way. The use case explored in detail was insurance dashboard, which aims to collect and show a consumer in a user-friendly way their different insurance policies and related information at a single glance, aggregating and combining information from the various insurance companies/intermediaries each consumer could have business with. Additionally, such a dashboard can integrate the functionalities of a comparison tool, enabling the consumer to compare coverages and prices between existing providers and others on the market.

Any information from the consumer would only be visible to players other than ones with which the consumer has a specific contract if the consumer explicitly requires it. If all information were available, it would allow the

[4] See EC (2023) COM(2023) 360 final.

consumer to see his full insurance position and also see alternative offers and compare products so as to make an informed choice. This can be seen as an alternative for more digital consumers to have access to all relevant information in a meaningful and consumer-focused way. The logic is that from a consumer perspective the complexity of many insurance products makes it difficult for consumers to understand their overall insurance situation such as what insurance policies they have, what is covered by their existing insurance policies, what is excluded and where they might have personal protection gaps. Currently consumers are not able to access a single overview of their existing insurance policies in a non-cumbersome way unless they have consolidated these insurances in one place (e.g. using one broker or one undertaking for all their insurance policies).

It should be highlighted that consumers should always have control over the data and their flows/permissions, i.e. the consumer may decide that only he/she sees the full information, allows certain undertakings/brokers to see all the information or have it completely open.

Exploring an insurance dashboard use case includes the need to focus on areas such as the data flows involved, potential roles and responsibilities of different stakeholders, the application of existing legal frameworks, implementation challenges and risks regarding data sharing, and potential concrete benefits and risks for consumers.[5]

From data accessibility and availability a prospective insurance dashboard requires product information (risks covered, exclusions, price, duration of the contract, provider name etc.), customer identification information (name, surname, address, phone, email, date of birth, place of birth) and information on insurable assets (varying according to line of business). All this information is currently available in insurer or intermediary databases or in the public domain. However, most of the data that is needed for the use case, despite being available, is not accessible for re-use. Insurers and intermediaries are not obliged to make these data available to other insurers or third parties in machine-readable and standardised format (e.g. through APIs). There is no legal requirement for this [except the General Data Protection Regulation (GDPR) data portability rule, which covers only certain data and is not in practice operational].

Hence, currently developing dashboard services involves leveraging PSD2 data, web scraping, the consumer taking the initiative to provide data or bilateral negotiations, agreements and contracts, and working to bridge different

[5] For more detail see EIOPA (2023).

standards since there is insufficient interoperability (standardisation). Given this, for an insurance dashboard to be more efficient and lead to the expected benefits it would need to have at least a certain level of standardisation of data and products and possible compulsory data sharing requirements for the insurance industry based on the explicit consent of the customer.[6] The data to present to the users in the dashboard can either be stored centrally or the dashboard can connect to the data providers each time a user has been authenticated and identified (and delete the data from its system after the user has logged off).

The sharing of and access to consumer data in an open insurance context must take place in a transparent, safe and ethical environment in full respect for all EU data protection requirements. When building such a dashboard it should be ensured that consumers fully understand what they are consenting to and potential risks related to overall information overload and complexity stemming from poorly designed consumer journeys should be mitigated.

The workshop participants also explored possible benefits and risks in relation to the use cases that have been identified. Data protection, security issues and the question of exclusion or discrimination were the major concerns highlighted. The more information insurance undertakings have about a given individual, the greater the probability that some parameter or combination of parameters could negatively affect the coverage or pricing that individual gets. Exclusions may not only come as a result of excessive data. Coverage might be denied to people who are unwilling to share certain information. Those that are not very tech-savvy and do not use modern devices might be left behind because of a lack of analysable data or other barriers. A potential increase in ICT and cyber risk and a potential lack of control over personal data were also highlighted.

The use case discussion concluded that in the broadest sense the development of open insurance products or services might lead to benefits for consumers (e.g. in terms of personalised pricing, increased competition, better access to insurance, fraud detection), but it also raises risks such as the exclusion of classes of customers due to their risk profile, mis-selling, increased information asymmetry against consumers and price discrimination. In addition, data protection and confidentiality issues, even if not strictly under the remit of prudential and conduct supervisors, become more relevant. As such, development needs to be monitored, emergent risks identified and where regulatory adjustments and supervisory responses are necessary they should be considered.

[6] Note that the FIDA proposal that was published after the workshop aims to solve some of these issues.

4. Collaborative analytics in transaction monitoring

The amount of money laundered worldwide is estimated to be between 2% and 5% of global GDP.[7] Only an insignificant portion of it is recovered. The fight against money laundering is essential, and the EU is engaged in it on several fronts. Under the Anti-Money Laundering Directive,[8] obliged entities must conduct ongoing monitoring of their business relationships, including transaction monitoring. RegTech solutions are increasingly popular in this respect.

During the EU-SDFA RegTech workshop several examples were presented. Among them was a solution for transaction monitoring that served as a basis for a subsequent discussion on data sharing and collaborative analytics. In this example, several banks joined forces to improve the identification and utility of unusual transaction reports to financial intelligence units (FIUs). More specifically, the main added value of this use case results from the fact that it puts together encrypted customer transaction data from participating banks to identify patterns and uncover possible transaction networks that would not be visible to any single bank. When such unusual patterns are detected, the participating banks receive an alert, investigate on their side, and report to the FIU when required.

It should be noted that in this setup, the banks remain solely responsible for monitoring transactions and for the business relationship with the customers.

It is important to highlight that to ensure data protection not all customer data is shared, but only those parts that are necessary for the monitoring activity, and sensitive data is pseudonymised before sharing using privacy-enhancing techniques. This means that the data cannot be directly linked to the customer by other parties because only the bank has the encryption/decryption key. The shared data include business identifiers and a subset of transaction information, for example the time, amount and destination of the transaction. In addition, at the moment only business customers' data and transactions are handled, i.e., there is no natural persons' data processed. The overall process is set up in such way that the participating banks are not sharing the same set of data among themselves but are only sharing the pseudonymised data with the entity tasked with the analysis.

[7] See Europol money laundering page and UN Tax abuse, money laundering and corruption article

[8] Directive (EU) 2015/849.

Regarding the security of the data, several measures are applied. In particular, all actions and data processing activities, including search actions, are recorded and can be traced back to the individual employees.

Various machine learning models and statistical techniques are used to gain new insights from the pooled data. In terms of performance, the machine learning-based models produced significantly better results than the rule-based tools.

The case study highlighted an interesting approach and set the stage for a subsequent discussion regarding possibilities of using different technologies and data collaboration in the fight against money laundering.

To further improve the benefits that can be derived from such analysis, one of the ideas discussed was to link to the natural persons' data, for example about the ultimate beneficiaries or the directors of companies and proceed using a similar methodology to the case study mentioned. While this would help reveal further networks and relationships between firms, it also brings challenges related to data protection. Indeed, financial institutions have an interest in acting as financial gatekeepers fighting financial crime, and the benefits of a larger data set to detect financial crime networks are undeniable. The same benefits have also been observed by several AML supervisors and FIUs having engaged in similar endeavours at national and cross-border levels.

A proof of concept, Aurora,[9] uses a similar approach to the one in the case study, trying out centralised and decentralised privacy-enhanced collaborative data analytics at the national and cross-border levels. It also concludes that the collaborative machine-learning approach yields superior results to the siloed rule-based approach. However, in other projects, supervisors[10] faced the same issues as the private sector, e.g., needing more legal clarity on data privacy and confidentiality matters, including when using external resources to build analytics tools.

Keeping in mind the potential negative consequences of sharing personally identifiable information is also necessary. For example, involving more intermediaries could also mean a greater risk of data breaches. In this case, as these processors would be using multiple large data sets, they could become a preferred target for cybercriminals, especially if major players emerge among these processors.

[9] See BIS (2023).

[10] See BIS (2019).

Another question that was raised is regarding the potential consequences for the business relationship between the bank and its customers because of the triggered alerts and whether this would lead to service denial without a full background in some cases (i.e., false positives based on data that the bank facing the customer cannot verify or did not vet). Although, in the example studied, this could be mitigated by having humans in the loop and by the fact that participating banks fully investigate alerts and do not base their decisions solely on the signals received, mitigants for such issues need to be embedded by design in the case of potential future use of automated solutions.

In addition, it is only fair to exhaustively consider all the alternative approaches available in terms of technologies, as it is possible that other solutions might present better trade-offs or lower risks. Suggestions for alternatives included zero-knowledge protocols. There are also other technological alternatives such as confidential computing, multi-party secure computations and governance options including the nature of the parties' responsibilities and public-private partnerships.

In conclusion, this use case and the discussion highlighted interesting approaches to data sharing and collaboration that could benefit the fight against money laundering. The initial results from various experiments are promising, but these approaches bring additional risks and there is still legal uncertainty in some areas. In essence, one needs to keep an open yet critical mind to ensure that data protection rights are preserved and that regulatory objectives are achieved while maintaining technological neutrality.

Creating awareness of the uses and limitations of different privacy-enhancing techniques, collaborative analytics and secure computation techniques (including hardware solutions) among supervisors could be a sensible place to start for a better and holistic understanding of the full picture. There is a need to have a more precise cost-benefit analysis and to consider in more depth a more exhaustive range of techniques and governance settings to share and analyse data. Such efforts might be more targeted and effective if the industry is included as a partner in this endeavour to help focus on the most important practical issues.

5. Conclusion

From different points of view, the use cases presented in this chapter offer insights into how deeply embedded digitalisation and technology have become in financial services – and inevitably in their supervision. These use cases demonstrate particularly well the value to supervisors and regulators of coming to grips with the many aspects and implications of an increasingly technological and digitalised financial sector.

References

BIS (2019) Bank for International Settlements. *SupTech applications for anti-money laundering*. FSI Insights on policy implementation No 18. Available here.

BIS (2023) Bank for International Settlements. *Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders.* Available here.

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 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.

EC (2023) European Commission. *Proposal for a Regulation of the European Parliament and the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554*. COM(2023) 360 final.

EIOPA (2023) European Insurance and Occupational Pensions Authority. *Discussion paper on Open Insurance: an exploratory use case in the insurance sector*. EIOPA-BoS-23-211, 24 July 2023. Available here.

ESMA (2022a) European Securities and Markets Authority. *Parsing prospectuses: A text-mining approach.* ESMA TRV Risk Analysis, 29 November 2022. Available here.

ESMA (2022b) European Securities and Markets Authority. *Peer review of the scrutiny and approval procedures of prospectuses by competent authorities*, ESMA 42-111-7170, 21 July 2022. Available here.

Publications Office
of the European Union

ISBN:978-92-9466-490-7
doi:10.2870/51343
QN:QM-02-23-285-EN-N

Funded by
the European Union