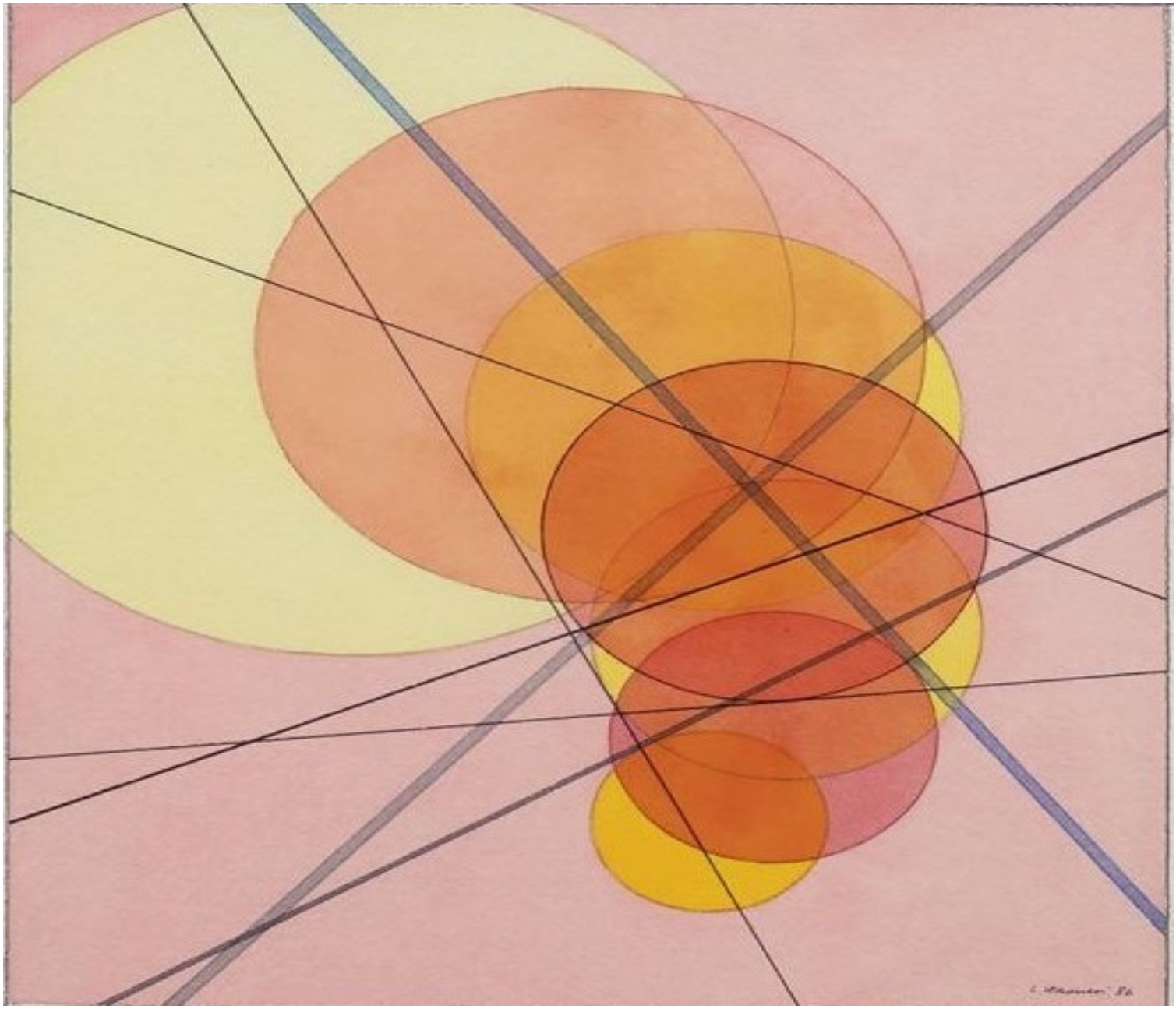
Issue N. 26 - 2024

ARGO

New Frontiers in Practical Risk Management



iason
ESSENTIAL SERVICES FOR
FINANCIAL INSTITUTIONS

iason

Argo magazine

Year 2024 - Issue Number 26

Published in July 2024
First published in October 2013

Last published issues are available online:
http://www.iasonltd.com

Front Cover: **Luigi Veronesi**, *Geometrie*, 1986.

Milan Headquarter:
Corso Europa, 15
20122 Milan
Italy

London Headquarter:
3rd Floor, 120 Baker Street
W1U 6TU London
United Kingdom

Madrid Headquarter:
Calle Miguel Ángel, 16
28010 Madrid
Spain

Contact Information:
info@iasonltd.eu
www.iasonltd.com

iason is a registered trademark.

Articles submission guidelines
Argo welcomes the submission of articles on topical subjects related to the risk management. The articles can be indicatively, but not exhaustively, related to models and methodologies for market, credit, liquidity risk management, valuation of derivatives, asset management, trading strategies, statistical analysis of market data and technology in the financial industry. All articles should contain references to previous literature. The primary criteria for publishing a paper are its quality and importance to the field of finance, without undue regard to its technical difficulty. Argo is a single blind refereed magazine: articles are sent with author details to the Scientific Committee for peer review. The first editorial decision is rendered at the latest within 60 days after receipt of the submission. The author(s) may be requested to revise the article. The editors decide to reject or accept the submitted article. Submissions should be sent to the technical team (**info@iasonltd.eu**). LaTeX or Word are the preferred format, but PDFs are accepted if submitted with LaTeX code or a Word file of the text. There is no maximum limit, but recommended length is about 4,000 words. If needed, for editing considerations, the technical team may ask the author(s) to cut the article.

Table of Contents

Dear Readers,

Welcome to the summer edition of Argo Magazine, an issue with heterogeneous contents on some of the most interesting and cutting-edge themes that will involve banking institutions in the near future.

Indeed, you can start with the session dedicated to Iason Just in Time, reading our overviews and analysis on the new ECB guide on internal model and on the document Digitization of Finance" published by BIS, crucial for outlining best practices and the implications of fintech developments for banks and banking supervisors.

*The iason Research Papers session follows with the Technology section dedicated to an analysis of the "**Artificial Intelligence Act**" (by D. Esposito, P. Carrozzino and B. Ghilardi), the European regulation that establishes a uniform legal framework for the development, placing on the market, putting into service, and use of artificial intelligence systems to promote the uptake of human centric and trustworthy AI while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of fundamental rights of the European Union.*

*The second article we propose is "**Exploring the Digital Renminbi: Insights into China's CBDC**" by G. Mori et al., which revisits the topic of Central Bank Digital Currencies (CBDC) discussed in the Argo Collection last December, focusing, this time, on the distinctive characteristics and potential applications of the Chinese Digital Renminbi.*
The document begins with a comprehensive overview of the evolution of the e-CNY development, and then delves into the design of its architectural model, exploring its distribution model, the key principles underlying Digital Wallets, and the technological framework supporting the Chinese CBDC.
Lastly, the paper introduces the paradigm of cross-border payments with mBRIDGE, an initial project and then a real exchange platform where the international involvement of participants has acted as a sounding board to raise awareness of the collaboration between central banks, commercial banks, and corporate institutions.

*The issue closes with "**Introducing sectoral PD satellite models through constrained BACE**" by A. Mauri, R. Di Sivo and R. Greco. The authors propose a methodology for estimating sector-specific satellite PD models that can be consistently used to conduct scenario analyses based on specific sector shocks, such as the EU-wide stress test exercises of the EBA and climate-related scenarios.*
In particular, the Bayesian average estimation approach known as BACE is comple-

mented by a study of the relative importance of estimators in terms of Dominance Analysis, which aims to estimate models with sufficient sensitivity to the driver of the sectoral scenario, identified as Gross Value Added (GVA).
This leads to a methodological framework that can be used for any type of sectoral analysis involving GVA scenarios.

We conclude suggesting you visit our online Research page and subscribe to our newsletter service with a monthly update on the most relevant topics about practical Risk Management.

We wish you a happy reading and a relaxing summer break!

Antonio Castagna
Luca Olivo
Giulia Perfetti

Just in Time

iason Notes

ECB Guide to Internal Models 2024: General Topics and Credit Risk

On 19 February 2024, the European Central Bank (ECB) published its final revised Guide to internal models, following a public consultation which ended in September 2023. The Guide explains how the ECB understands the rules banks must follow when they use internal models. The purpose of this JIT is to offer an overview regarding the ECB's understanding of various subjects related to general topics and internal models used in calculating own funds requirements for credit risk. The revisions to the Guide clarify how banks should go about including material climate-related and environmental risks in their models.

read more

Date July 2024

ECB Guide to Internal Models 2024: Market Risk

On 19 February 2024, the European Central Bank (ECB) published its final revised Guide to internal models, following a public consultation which ended in September 2023. The Guide explains how the ECB understands the rules banks must follow when they use internal models. The purpose of this JIT is to offer transparency regarding the European Central Bank's (ECB) understanding of various subjects related to internal models used in calculating own funds requirements for market risk. It is important to clarify that this chapter does not aim to comprehensively cover all topics that could be subject to review during internal model investigations, such as model governance.

read more

Date July 2024

ECB Guide to Internal Models 2024: Counterparty Credit Risk

This presentation aims to provide an overview of both the Counterparty Credit Risk (CCR) chapter of the new version of the ECB guide to internal models published by the European Central Bank in February 2024 and of the consultation on Guidelines for counterparty credit risk management issued by the Basel Committee on Banking Supervision (BCBS). The intent of the first document is to provide transparency regarding the ECB understanding about some of the principles defined for the Internal Model Method (IMM) in the Capital Requirements Regulation (CRR), that is Regulation (EU) No 575/2013 of the European Parliament and of the Council.

read more

Date July 2024

Digitalisation of Finance: Regulation, Risks and Opportunities

Digitalisation is radically transforming the banking sector and has enabled technological trends to be used to take advantage of them, seeking to understand the implications for banks and banking supervision and to issue standards or guidelines to mitigate emerging risks.

The "Digitalisation of Finance" document published by the Bank for International Settlements (BIS) partly builds on the paper from 2018, “Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors”, published by the Basel Committee on Banking Supervision (BCBS).

read more

Date July 2024

EBA Report on the 2023 Credit Risk Benchmarking Exercise

On April 2024, the European Banking Authority (EBA) published its annual benchmarking exercise, aims to monitor the variability of the RWAs for institutions applying the IRB approaches in EU Member.

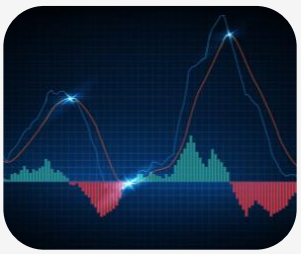
The report shows the evolution of the variability of the risk parameters over the period 2015-2023.

A clear decreasing trend of variability can be observed in the Corporates class, whereas for the other asset classes the variability seems more stable.

read more

Date May 2024

EBA Report on the 2023 Market Risk Benchmarking Exercise



The report presents the results of the 2023 supervisory benchmarking exercise according to the article 78 of the Capital Requirement Directive (CRD) and the related regulatory and implementing technical standards (RTS and ITS) that define the scope, procedures and portfolios for benchmarking internal models for market risk (MR).

The report summarizes the conclusions drawn from a hypothetical portfolio exercise (HPE) conducted by the EBA during the 2022/2023.

read more

Date May 2024

Behavioral Modelling and ALM - A Scenario Analysis on the Spanish Banking System

In December 2023, the Basel Committee (BSBC) aims to propose a new methodology for calculating interest rate shocks in the Interest Rate Risk in Banking Book (IRRBB) framework.

This JIT aims to perform a scenario analysis of the impact of the Supervisory Outlier Tests, (from now on SOT). We present a 5-year scenario analysis carried out on Spanish data that allows us to appreciate the characteristics of Iason's behavioral models for managing non-maturing deposits.

read more

Date July 2024

iason Weekly Insights

Regulatory/Supervisory Pills

Among iason's various publications we also find the iason Pills.

With these daily Pills, iason aims to offer a summary on information, mostly, of the main regulatory and supervisory news in the banking and finance sector on both Pillar I and Pillar II risks of the Basel framework. The main purpose of these publications is to give the reader an effective, timely and brief overview of the main topics of the moment.

The author of the Iason Pills is Dario Esposito.

Subscribe to our Pills newsletter.

read more

Market View

Among iason's weekly insight you can also find the iason Market View, a weekly update on financial market by Sergio Grasso.

The author, with almost three decades of investment experience, presents an accurate analysis of market fluctuations of the week, giving a critical view of observed phenomenos and suggesting interesting correlations with the main world events.

Subscribe to our Market view newsletter.

read more

GOVERNANCE. METHODOLOGY. TECHNOLOGY.

iason is a company specialised in advanced solutions for the **Risk Management** of **Financial Institutions.**

We provide highly qualified **consulting services** in the **methodological** and **technological** fields, together with targeted support for **Data** and **Model Governance** projects in risk frameworks.

We strongly believe in **Research** because we want to guarantee our clients services and solutions that are always at the forefront of **Regulatory** and **Modelling** requirements.

ARGO MAGAZINE

Quarterly magazine on the new frontiers of Risk Management

RESEARCH PAPER SERIES

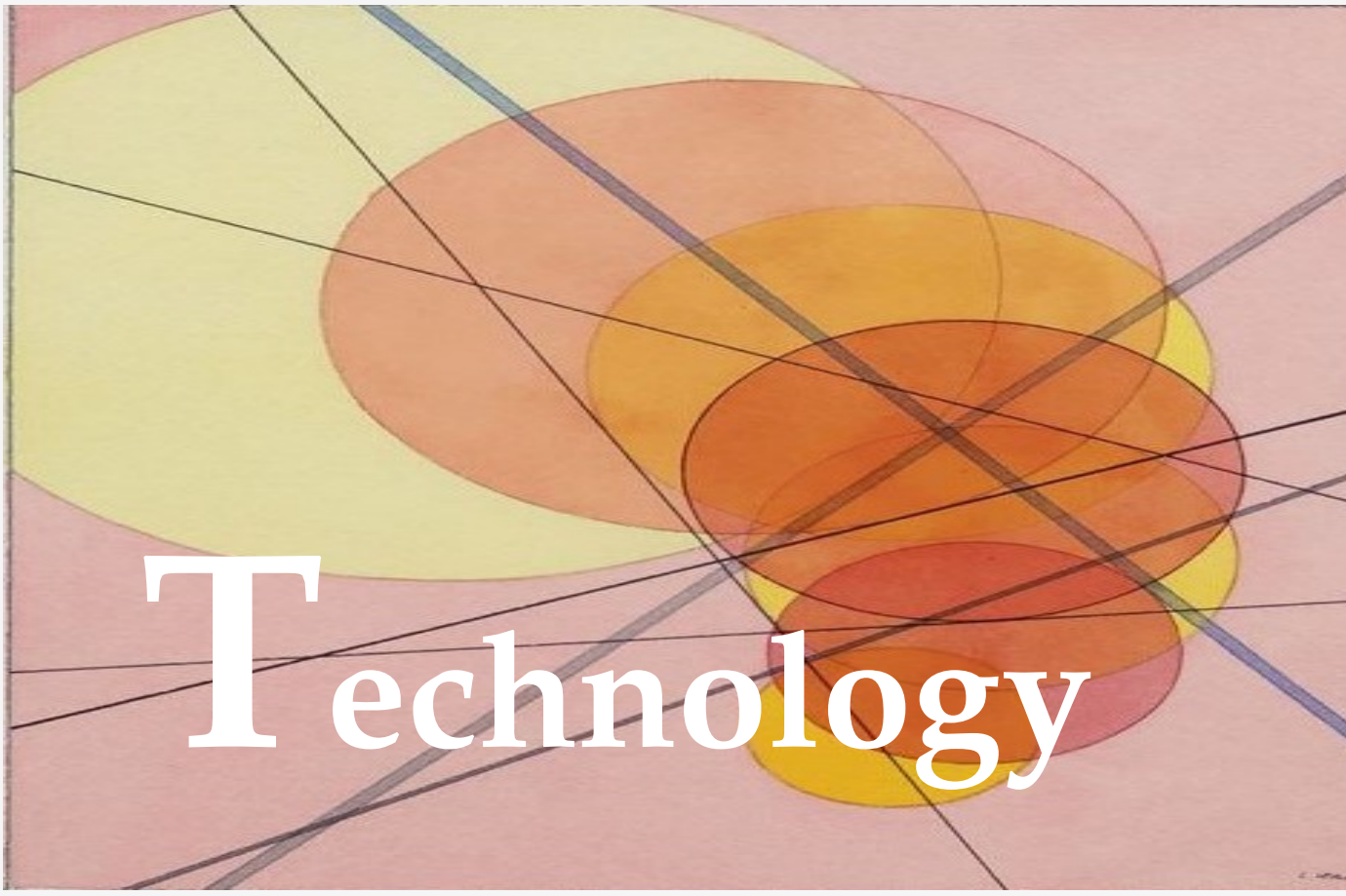
Research articles on innovative and advanced methodologies in the financial sector

JUST IN TIME

Real-time updates on regulatory changes

FOLLOW US!

iason ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS



Artificial Intelligence Act (AI Act)

About the Authors

Dario Esposito:
Chief Risk Regulatory Officer
Experienced professional with a demonstrated history of working in the financial services industry. Skilled in Enterprise Risk Management, Basel III and IV and AML. Strong finance professional postgraduated from University of London and IMD in Lausanne (International Institute for Management Development).

Pierpaolo Carrozzino:
Business Analyst
He holds a master's degree in Intermediaries, International Finance, and Risk Management from Sapienza University of Rome. He worked in the Banking Regulation sector for a year and then moved to the risk management field. Currently, he has been working on the Risk Data Aggregation and Risk Reporting (RDARR) project in one of the major Italian banks.

Bianca Ghilardi:
Business Analyst
She holds a master degree in Management and Finance from Universitá del Piemonte Orientale in Novara. After a few months in the IT sector as tester engineer, she moved to the risk management field. Actually, she is working in a Model Risk Management project in one of the largest Italian banks.

This document was prepared in collaboration with Matteo Cecchin, who at the time was working for Iason Consulting.

Artificial Intelligence Act (AI Act)

Dario Esposito Matteo Cecchin Pierpaolo Carrozzino Bianca Ghilardi

The purpose of Artificial Intelligence Act *(AI Act) is to improve the functioning of the internal European market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of AI systems to promote the uptake of human centric and trustworthy AI while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of fundamental rights of the European Union.*
The Act seeks to balance the drive for technological innovation and emphasizes the need to prevent the fragmentation of the internal market due to divergent national regulations, thus facilitating the free movement and cross-border deployment of AI-based goods and services.

Artificial Intelligence (AI) is a fast-evolving family of technologies that contributes to a wide array of economic, environmental and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of AI can provide key competitive advantages to undertakings and support socially and environmentally beneficial outcomes. At the same time, depending on the circumstances regarding its specific application, use, and level of technological development, AI may generate risks and cause harm to public interests and fundamental rights that are protected by European Union law.
AI systems can be easily deployed in a large variety of sectors of the economy. Certain Member States have already explored the adoption of national rules to ensure that AI is trustworthy and safe and is developed and used in accordance with fundamental rights obligations. Diverging national rules may lead to the fragmentation of the internal market and may decrease legal certainty for operators that develop, import or use AI systems. With the Artificial Intelligence Act (AI Act) Regulation, however, a high and consistent level of protection is guaranteed throughout the European Union can therefore be ensured in order to achieve trustworthy AI, while divergences hampering the free circulation, innovation, deployment and the uptake of AI systems and related products and services within the internal market can be prevented by laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market.
In particular, in the banking sector the use of AI by operators is generating a series of changes that will have an impact, sometimes radical, on various profiles: on customers through a modification of their purchasing experience; on the productivity of operators through a change in production processes and the value chain; for the authorities, following the review of risk measurement and management techniques and the implications for supervisory tools. As regards use cases, there are many applications in the banking sector: from marketing to combating fraud in transaction banking and payments, from scoring models for credit risk to risk management systems[2].

The Artificial Intelligence Act (AI Act)

On 21 April 2021[9], the Commission presented a proposal for a regulation aimed at harmonizing the rules on artificial intelligence (AI Regulation) and a coordinated plan comprising a series of joint actions for the Commission and Member States. This package of rules aimed to increase trust in AI and promote the development and upgrading of AI technologies. On December 2022[4], the European Council has adopted its common position (*"general approach"*) on the AI Act and in June 2023[12], the European Parliament has adopted their negotiation position for the draft AI Act. On 9 December 2023[10], the Council and Parliament reach a provisional agreement on the AI Regulation after months of negotiations. **During 2024, both the Council** (21 May 2024[11]) **and the Parliament** (13 March 2024[13]), **as EU co-legislators, formally adopted the final text**. The AI Act will therefore enter into force on the twentieth day following its publication in the Official Journal of the EU and will be fully applicable after 24 months. However, some specific provisions will have different application dates, such as bans relating to AI systems with an unacceptable level of risk, which will be applicable starting 6 months after entry into force, or provisions relating to GPAI models already in place on the market, for which a deadline of 12 months is envisaged to guarantee compliance with the provisions of the Regulation (for further details please refer to the chapter "Entry into force and review").
The purpose of the AI Act Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter of Fundamental Rights, including democracy, the rule of law and environmental protection, against the harmful effects of artificial intelligence systems (AI systems) in the European Union, and to support innovation. To achieve that objective, rules regulating the placing on the market, the putting into service and the use of certain AI systems was laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit

from the principle of free movement of goods and services. Those rules are clear and robust in protecting fundamental rights, supportive of new innovative solutions, enabling a European ecosystem of public and private actors creating AI systems in line with EU values and unlocking the potential of the digital transformation across all regions of the EU. By laying down those rules as well as measures in support of innovation with a particular focus on small and medium enterprises (SMEs), including startups, this Regulation supports the objective of promoting the European human-centric approach to AI and being a global leader in the development of secure, trustworthy and ethical AI as stated by the European Council.
In the AI Act, an *"AI system"* is considered a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. This notion of "AI system" is closely aligned with the work of international organisations working on AI to ensure legal certainty, facilitate international convergence and wide acceptance, while providing the flexibility to accommodate the rapid technological developments in this field. Moreover, it is based on key characteristics of AI systems that distinguish it from simpler traditional software systems or programming approaches and not cover systems that are based on the rules defined solely by natural persons to automatically execute operations.
The techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic - and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved. The capacity of an AI system to infer transcends basic data processing, enables learning, reasoning or modelling.
In order to obtain the greatest benefits from AI systems while protecting fundamental rights, health and safety and to enable democratic control, AI literacy[1] must equip providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI systems. AI literacy must provide all relevant actors in the AI value chain with the insights required to ensure the appropriate compliance and its correct enforcement.
Also, in order to ensure a level playing field and an effective protection of rights and freedoms of individuals across the European Union, AI Act it also recognizes the importance of international cooperation, aiming for regulatory consistency and fostering global dialogue on ethical AI standards. The regulation applies in a non-discriminatory manner broadly to AI systems' providers, deployers, importers, distributors, and manufacturers within the EU and those from third countries whose AI outputs are used in the EU. Furthermore, it explicitly includes provisions for authorized representatives and affected persons in the European Union.
The introduction of AI Act previews the Act's innovations, including measures to support AI innovation, particularly for SMEs, and the establishment of an EU database for high-risk AI systems. It also outlines proposed amendments to integrate the Act's requirements with existing EU legislation, ensuring a cohesive and comprehensive regulatory landscape.
As already reported above, AI can bring numerous benefits for society and the economy but, at the same time, it can also present risks for rights, security and the proper functioning of the single market. To find a balance between the two instances, the AI Act was designed with a risk-based approach. The regulatory framework on AI therefore provides for a classification of AI systems based on the level of risk they present for people and society. The framework distinguishes between four categories of risk: unacceptable, high, limited and minimal (as shown in the Figure 1):

- AI systems that pose an **unacceptable risk** are those that contradict fundamental EU values and principles, such as respect for human dignity, democracy and the rule of law. These systems are banned or (in the case of real-time biometric surveillance for security reasons) subject to severe restrictions. For example, AI systems that manipulate human behavior in a way that circumvents the will of users, or that enable *"social scoring"*[2] by public authorities are prohibited.
- AI systems that present a **high risk** are those that can have a *"systemic"* impact, i.e. a significant impact on the fundamental rights or safety of people. These systems are subject to rigorous obligations and requirements before they can be placed on the market or used. For example, this category includes AI systems used to evaluate the credit score or creditworthiness[3] of natural persons and the selection and recruitment of personnel, for admission to education, for the provision of essential social services, such as healthcare, for remote biometric surveillance (not in real time), for judicial and police applications, or for the management of critical infrastructure security.
- AI systems that present **limited risk** are those that can influence the rights or wishes of users, but to a lesser extent than high-risk systems. These systems are subject to transparency requirements, which allow users to be aware that they are interacting with an AI system and to understand its characteristics and limitations. For example, AI systems used to generate or manipulate audiovisual content (such as deepfakes), or to provide personalized suggestions (such as chatbots) fall into this category. There is a right to know that you are talking to a bot (instead of a human) and that that image is created or contrived by AI.
- AI systems that pose **minimal risk** are those that

[1] "AI literacy" means skills, knowledge and understanding that allows providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause.

[2] Systems aimed to classify or evaluate people or groups of people 'based on their social behavior or known or predicted personal or personality characteristics' resulting in a "social score" to the detriment of these people. These AI-based practices open or restrict access to social benefits and/or differentiate treatment based on a score obtained from assessing personal behaviors or attributes.

[3] AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems; AI systems used for those purposes may lead to discrimination between persons or groups and may perpetuate historical patterns of discrimination, such as that based on racial or ethnic origins, gender, disabilities, age or sexual orientation, or may create new forms of discriminatory impacts. However, AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under this Regulation.

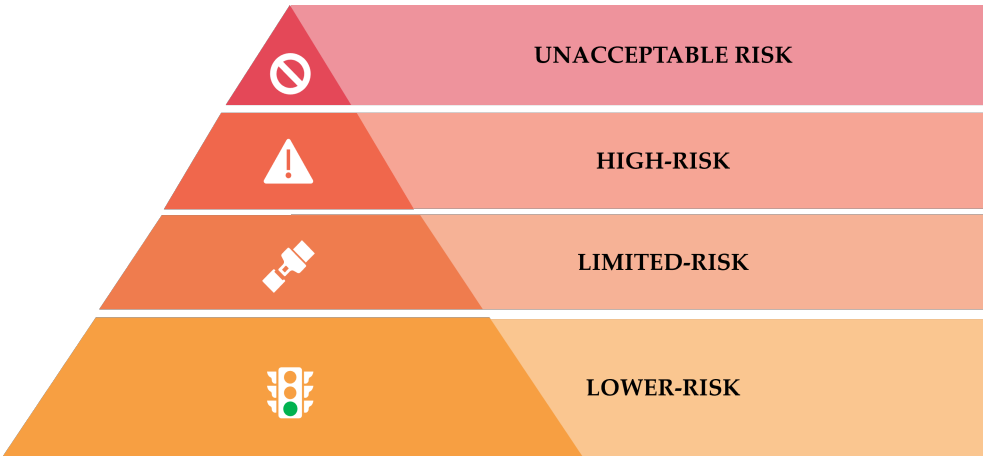


FIGURE 1: AI Act risk-based approach

have no direct impact on fundamental rights or the safety of people, and that offer wide margins of choice and control to users. These systems are free from any regulatory obligations, in order to encourage innovation and experimentation. For example, AI systems used for recreational purposes (such as video games) or for purely aesthetic purposes (such as photographic filters) fall into this category.

Among others, the following systems are excluded from the obligations of the AI Act Regulation:

- AI systems used exclusively for military, defense, or national security purposes;
- Public authorities and international organizations using AI in law enforcement and judicial cooperation, provided there are adequate safeguards for fundamental rights;
- AI systems developed solely for scientific research;
- AI systems or models before their market introduction or service provision;
- Personal, non-professional use of AI systems by natural persons.

Even through the risk-based approach is the basis for a proportionate and effective set of binding rules, it is important to recall the *"2019 Ethics guidelines for trustworthy AI"*[8] developed by the High-Level Expert Group (HLEG) on AI. In those guidelines, the AI HLEG developed seven non-binding ethical principles for AI which are intended to help ensure that AI is trustworthy and ethically sound. The seven principles include human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being and accountability. Those guidelines contribute to the design of a coherent, trustworthy and human-centric AI, in line with the Charter and with the values on which the European Union is founded.
In the continuation of the examination of this paper the focus is almost exclusively on the first two risk categories: *Prohibited AI practices* and *High risk AI system*.

Prohibited AI Practices

As already indicated before, AI Act outlines specific AI practices that are deemed unacceptable and are thus prohibited under the Act; this represents a crucial component of the EU's regulatory approach towards ensuring that the development and application of AI technologies align with fundamental rights, ethical standards, and societal values. The prohibited practices target AI systems that could potentially harm individuals' autonomy, safety, privacy, and rights, emphasizing the EU's commitment to a human-centric AI approach.
Primarily, the regulation explicitly bans AI systems that deploy **subliminal, manipulative, or deceptive techniques capable of materially distorting a person's behavior by impairing their ability to make informed decisions**. This prohibition targets AI systems that, through manipulation beyond a person's consciousness, could cause significant harm by leading individuals to make choices they would not have otherwise made. The underlying concern here is the protection of individual autonomy and the prevention of exploitation through AI-driven manipulation.
Secondly, AI systems designed to **exploit the vulnerabilities of specific groups, including those defined by age, disability, or socio-economic status, are prohibited**. This provision aims to prevent AI from materially distorting the behavior of vulnerable individuals in a way that could cause significant harm. It reflects the EU's commitment to safeguarding the rights and well-being of all citizens.
In addition to the practices already listed, the Act prohibits AI systems that evaluate or classify groups or individuals based on their social behavior or predicted personal characteristics over time, leading to detrimental or unfavorable treatment. **Social scoring** systems, which could result in unfair, disproportionate, or unrelated consequences in various social contexts, are seen as antithetical to EU values, including respect for human dignity and equality before the law.
Moreover, prohibited are AI systems used for making risk assessments of individuals to **predict their likelihood of committing a crime based solely on profiling or personality traits**. This prohibition, however, does not extend to AI systems supporting human assessments in criminal investigations where the analysis is based on objective facts directly linked to criminal activity. The focus here is on preventing unjust or biased law enforcement practices that could undermine fundamental rights, such as the presumption of innocence.
The Act bans also the use of AI for untargeted scraping of **facial images to create or expand facial recognition databases**. This prohibition addresses privacy concerns related to mass surveillance and the unauthorized collection of biometric data, emphasizing the importance of consent and the protection of personal data. In addition to what has already been reported above, prohibited is also the use

of AI to **infer emotions in contexts such as the workplace and educational institutions**, except for medical or safety reasons. This prohibition aims to protect individuals from invasive assessments that could lead to discrimination or adverse consequences based on inferred emotional states.
Furthermore, the regulation bans AI systems that **categorize individuals based on biometric data to infer sensitive attributes**, such as race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. This prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement. This prohibition seeks to prevent discriminatory practices and protect individuals' privacy and fundamental rights, particularly in sensitive areas.
Finally, the use of **real-time remote biometric identification systems** by law enforcement in publicly accessible spaces is forbitten, unless and in so far as such use is strictly necessary for one of the following objectives:

- The targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as searching for missing persons.
- The prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack.
- The localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation, prosecution or executing a criminal penalty.

This provision balances the need for public safety with the protection of privacy and fundamental freedoms, establishing stringent conditions for the deployment of such technologies.
Detailed conditions under which the limited exceptions for the use of real-time remote biometric identification systems may be applied are also established. These include the requirement for a fundamental rights impact assessment, registration of the system in the EU database, and strict temporal, geographic, and personal limitations to ensure that the use is necessary, proportionate, and respectful of individuals' rights and freedoms. The deployment of real-time remote biometric identification systems must be preceded by authorization from a judicial or independent administrative authority, ensuring oversight and accountability. In urgent situations, temporary use without prior authorization is permitted, provided that authorization is sought immediately thereafter. Member States have the discretion to authorize the use of real-time remote biometric identification systems within the framework set by the Act, reflecting the principle of subsidiarity and allowing for national variations in implementation. Each use of real-time remote biometric identification systems must be notified to relevant authorities, including market surveillance and national data protection authorities and Member States are required to report annually on the use of such systems; the Commission is tasked with publishing aggregated reports, ensuring transparency and public accountability.

High-Risk AI System

The regulatory framework for the classification, assessment, and management of AI systems deemed to be of high risk aims to ensure that **high-risk AI systems** are developed, deployed, and used in a manner that respects fundamental rights, ensures safety, and fosters trust among users and the broader public. In the AI Act, an *"high-risk"* is considered when the following conditions are fulfilled:

- The AI system is intended to be used as a safety component;
- The AI system is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product;
- The AI system is always considered to be high-risk where performs profiling of natural persons.

Otherwise, an AI system shall not be considered to be high-risk if it does not pose a significant risk of harm to the health, safety, or fundamental rights of natural persons, including by not materially influencing the outcome of decision making. This shall be the case where it performs a narrow procedural task, improves the result of a previously completed human activity, detects decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review and carrying out a preparatory activity for a purpose-relevant evaluation.

The use-cases of high-risk AI systems could be modified from European Commission when its purposes pose a risk of harm to health and safety, or an adverse impact on fundamental rights. When assessing the condition, the classification rules take into account the following criteria:

- The intended purpose;
- How much is involved within the process;
- The nature - i.e., the presence of special categories of personal data are processed - and amount of the data processed and used by the AI system;
- How autonomous the system acts and the possibility for a human to override a decision or recommendations that may lead to potential harm;
- The extent to which the use of an AI system has already caused harm to health and safety, has had an adverse impact on fundamental rights or has given rise to significant concerns in relation to the likelihood of such harm or adverse impact;
- The intensity of such harm or such adverse impact on a single or a multiple person;
- How important is the result achieved by the AI system despite the negative impact;
- How much is the imbalance between those negatively affected by the AI system and those who employ it;
- The extent to which the outcome produced involving an AI system is easily corrigible or reversible, taking into account the technical solutions available to correct or reverse it, whereby outcomes having an adverse impact on health, safety or fundamental rights, shall not be considered to be easily corrigible or reversible;
- The magnitude and likelihood of benefit of the deployment of the AI system for individuals, groups, or society at large, including possible improvements in product safety;
- The extent to which existing EU law provides for:
  - Effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;
  - Effective measures to prevent or substantially minimise those risks.

Finally, the European Commission is granted the power to removing high-risk AI systems where both of the following conditions are fulfilled:

- The high-risk AI system concerned no longer poses any significant risks to fundamental rights, health or safety;
- The deletion does not decrease the overall level of protection of health, safety and fundamental rights under EU law.

High-risk AI systems must comply with specified requirements, considering their intended purposes and the state of the art in AI technologies. Providers are responsible for ensuring full compliance with applicable EU legislation, are responsible for high-risk AI systems and guarantee consistency, avoid duplications and minimise additional burdens. They also shall have a choice of integrating, as appropriate, the necessary testing and reporting processes, information, and documentation regarding their product. In order to be able to represent all the information mentioned above, it is necessary to have a continuous iterative process planned and managed throughout the entire lifecycle of the high-risk AI system. This document is called **risk management system**, is mandatory and requires regular systematic review and updating. In order to better intervene in its risk management, measurement and mitigation activities, it uses risk management measures that are effective in making the residual risk associated with each danger acceptable, as well as the overall residual risk of high-risk AI systems.
To this end it is necessary to have operators with adequate technical knowledge, as well as the experience, education and training expected and the ability to learn the context in which the system is intended to be used. Through the use of high-risk AI systems testing, it is possible to ensure that they function consistently, respecting the requirements and limits - previously defined parameters and adequate probabilistic thresholds - for their intended purpose. Moreover, high-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data subject to data governance and management; in fact, they shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose.
With regards to data, it is therefore important that correct data processing is carried out, all the following conditions apply:

- The bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data;
- Regarding the special categories of personal data are subject to more stringent treatments:
  - There are technical limitations on the re-use of the personal data, and state of the art security and privacy-preserving measures, including pseudonymisation;
  - There are measures to ensure that the personal data processed are secured, protected, subject to suitable safeguards, including strict controls and documentation of the access, to avoid misuse and ensure that only authorised persons with appropriate confidentiality obligations have access to those personal data;
  - They are not to be transmitted, transferred or otherwise accessed by other parties;
  - They are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first;
- The records of processing activities include the reasons why the processing of special categories of personal data was strictly necessary to detect and correct biases, and why that objective could not be achieved by processing other data.

All this information shall be insert in a technical documentation shall be drawn up before that high-risk AI system is placed on the market or put into service. Everything reported within it must be continuously verified - in terms of compliance with the requirements provided by national competent authorities - and kept updated.
For specific categories, for example SME or start-up, the Commission shall establish a simplified technical documentation form targeted at the needs of small and microenterprises. Record-keeping ensures a level of traceability and facilitates the monitoring of the functioning of a high-risk AI system. The logging capabilities shall provide, at a minimum:

- Recording of the period of each use of the system (start date and time and end date and time of each use);
- The reference database against which input data has been checked by the system;
- The input data for which the search has led to a match;
- The identification of the natural persons involved in the verification of the results.

In addition to drawing up technical documentation, it is required that this has certain transparency characteristics. Transparency is essential to ensure compliance with the involved supplier and operator obligations. The instructions for use in an appropriate format that allows concise, complete, correct, and clear information as well as relevant, accessible and comprehensible to deployers. Technical documentation, record keeping and transparency are important factors that allow an effectively overseen by natural persons during the period in which they are in use.
High-risk AI systems shall be designed and developed in such a way to facilitate being overseen by natural persons during the period in which they are in use. Human oversight shall aim to prevent or minimise the risks to health, safety or fundamental rights that may emerge when the system itself is used improperly. The oversight measures shall be commensurate with the risks, level of autonomy and context of use of the high-risk AI system. Human oversight is assigned and enabled for those who are able to:

- Properly understand the relevant capacities and limitations of the high-risk AI system and be able to duly monitor its operation, including in view of detecting and addressing anomalies, dysfunctions, and unexpected performance;
- Recognize automatically relying or over-relying on the output produced by the system ("automation bias");
- Correctly interpret the high-risk AI system's output, considering, for example, the interpretation tools and methods available;
- Intervene in the operation through its interruption with a procedure that allows the system to come to a halt in a safe state.

High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they per-

form consistently in those respects throughout their lifecycle. For achieve these levels of performance the Authorities, encourage, as appropriate, the development of benchmarks and measurement methodologies. The robustness of high-risk AI systems may be achieved through technical redundancy solutions (i.e., backup or fail-safe plans) and with mechanism resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities. Furthermore, continuous learning after being placed on the market or put into service shall be developed in such a way as to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (*"feedback loops"*), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures. The technical solutions to address AI specific vulnerabilities shall include, in addition to cybersecurity, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (*"data poisoning"*), or pre-trained components used in training (*"model poisoning"*), inputs designed to cause the AI model to make a mistake (*"adversarial examples"* or *"model evasion"*), confidentiality attacks or model flaws.
Concerning the responsibilities of parties involved in the lifecycle of high-risk AI systems the providers are subject to a range of obligations, including ensuring compliance with regulatory requirements, maintaining quality management systems. The tasks shall be kept in a comprehensive and systematic documentation and in an orderly manner in the form of written policies, procedures, and instructions. hey shall ensure the degree of rigor and the level of protection required by the Regulation, conducting necessary corrective actions (to withdraw it, to disable it, or to recall it, as appropriate):

- **Providers** when are established in third countries shall, prior to making their high-risk AI systems available on the European Union market, appoint an authorised representative which is established in the EU. The authorised representative, by written mandate, perform the same tasks that each provider is required to do (verify and provide the technical documentation and all the information necessary to demonstrate the conformity of high-risk AI system and reduce and mitigate every possible risk involved). The authorised representative shall terminate the mandate if it considers or has reason to consider the provider to be acting contrary to its obligations pursuant to the AI Regulation and inform the market surveillance authority of the Member State about the termination of the mandate and the reasons therefor.
- **Deployers** that use high-risk AI systems shall take appropriate technical and organisational measures to ensure - according to provided instructions - the human oversight shall be assigned to natural persons who have the necessary competence, training and authority, as well as the necessary support. They shall exercise the control over the input data and monitor the operation of the high-risk AI system, and, when they identify a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident. They are autorised to conserve the logs automatically generated of at least six months, unless provided otherwise in applicable EU or national law.
  Before putting into service or using a high-risk AI system at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. They also shall evaluate the high-risk AI systems' impact through assessment of the performs in terms of categories concerned (groups of person or specific risks), human oversight measures, internal governance, and complaint mechanisms; with the goal of taking the necessary steps to update the information and report any risks or incidents associated with the system's use.

Notifying authorities and notified bodies play a critical role in assessing and certifying the conformity of high-risk AI systems with regulatory requirements:

- **Notifying authorities**: each Member State shall designate or establish at least one notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation, and notification of conformity assessment bodies and for their monitoring. Those shall be organised in such a way that:
  - No conflict of interest arises with conformity assessment bodies, and that the objectivity and impartiality of their activities are safeguarded;
  - Decisions relating to the notification of conformity assessment bodies are taken by competent persons different from those who carried out the assessment of those bodies;
  - Offer or provide neither any activities that conformity assessment bodies perform, nor any consultancy services on a commercial or competitive basis;
  - Have at their disposal an adequate number of competent personnel at their disposal for the proper performance of their tasks.
- **Notified bodies**: there are individual that depend on neither any the provider of a high-risk AI system in relation to which they perform conformity assessment activities, nor any other operator having an economic interest in high-risk AI systems assessed, as well as of any competitors of the provider. Those shall satisfy the organisational, quality management, resources and process requirements that are necessary to fulfil their tasks, as well as suitable cybersecurity requirements.
  The organisational structure, allocation of responsibilities, reporting lines and operation of notified bodies shall ensure confidence in their performance, and in the results of the conformity assessment activities that the notified bodies conduct; in fact, they shall not engage in any activity that might conflict with their independence of judgement or integrity.
  Notified bodies shall have documented procedures in place ensuring that their personnel, committees, subsidiaries, subcontractors and any associated body or personnel of external bodies maintain the confidentiality of the information which comes into their possession during the performance of conformity assessment activities, except when its disclosure is required by law.
  Where a notified body finds that an AI system no longer meets the requirements taking account of the principle of proportionality, suspend or withdraw the certificate issued or impose restrictions on it, unless compliance with those requirements is ensured by appropriate corrective action taken by the provider of the system within an appropriate deadline set by the notified body.

For high-risk AI systems is important the presence of harmonized standards and common specifications. Providers can choose between various conformity assessment procedures to demonstrate compliance, depending on whether harmonized standards or common specifications are applied:

- **Standard request** is required by the Commission and serves to understand where improve AI systems' resource performance, such as reducing the consumption of energy and other resources during its lifecycle, and on the energy-efficient development of general-purpose AI models.
  Then goals during the standardisation process by the participants are to promote investment and innovation in AI, including through increasing legal certainty, as well as the competitiveness and growth of the EU market, contributing to strengthening global cooperation on standardisation and considering already existing international standards. The Commission is empowered to adopt, implement acts establishing common specifications in case harmonised standards have not been accepted, are not given within the deadline set, or do not follow fundamental rights, compliances, or requirements.
  The Act aims to ensure that high-risk AI systems are developed and used in a manner that upholds safety (conformity and compliance with cybersecurity), fundamental rights, and public trust. The provider shall have applied:
  - The internal controls; or
  - The assessment of the quality management system and the assessment of the technical documentation, with the involvement of a notified body.
- **EU declaration of comformity** shall identify the high-risk AI system for which it has been drawn up. That shall contain all the information required to identify the European Union harmonisation legislation to which the declaration relates. The provider - who has drawn up the EU declaration of conformity - shall assume responsibility for compliance with the requirements and keep the EU declaration of conformity up to date as appropriate.
  Before placing it on the market or putting into service a high-risk AI system the provider or another individual representative shall register themselves and their system in the EU database; these will be registered at national level.

Transparency Obligations for Providers and Deployers of Certain AI System

When natural persons interact directly with AI systems, it is **responsibility of providers** to inform them that they are interacting with an AI system especially in contexts where they generate or manipulate content, such as synthetic audio, image, video, or text. This could be taken for granted when is obvious from the point of view of a natural person who is reasonably well-informed, observant, and circumspect, taking into account the circumstances and the context of use or when AI systems are authorised by law for a specific reason (to detect, prevent, investigate or prosecute criminal offences).
The effectiveness, interoperability, robustness, and reliability of these technical solutions are crucial, considering the limitations of content types, implementation costs, and the state of the art in relevant technical standards. Exceptions include AI systems used for standard editing assistance or those that do not significantly alter deployer-provided data or its semantics, and systems authorized for law enforcement purposes. Because there are systems that can recognize emotions and biometric categorization systems, the **deployers** are obligated to inform individuals exposed to these systems about their operation, subject to appropriate safeguards for the rights and freedoms of third parties, and in compliance with EU law.
AI system that generates a *"deep fake"*, shall disclose that the content has been artificially generated or manipulated when it is created with the purpose of informing the public on matters of public interest. In addition, if the content forms part of an evidently artistic, creative, satirical, fictional analogous work or program, are allowed as long as the transparency obligations are appropriate and not hamper the display or enjoyment of the work. The obligations outlined on the AI technologies ensure that are utilized in a manner that is transparent, respectful of personal privacy, responsibly and consistent with fundamental rights.
The AI Office is tasked with encouraging the development of codes of practice at the EU level to aid in implementing these obligations effectively. The Commission has the power to adopt implementing acts to approve these codes or, if necessary, specify common rules for their implementation.

General-Purpose AI Models

General-purpose AI models are classified as having systemic risk based on their capabilities or impact. This classification is determined through technical evaluation, including indicators and benchmarks, or by a Commission decision following an alert from the scientific panel. A key quantitative threshold for classifying an AI model as having systemic risk is the use of computation exceeding $10^{\wedge}25$ floating-point operations (FLOPs) for its training. The Commission is empowered to adjust these thresholds and criteria to keep pace with technological advancements. The provider shall notify the Commission that their general-purpose AI models meet systemic risk criteria within two weeks of learning that it will be satisfy. That notification shall include the information necessary to demonstrate that the relevant requirement has been met; without it the Commission may decide to designate it as a model with systemic risk. Under request by provider, the AI System could be reassessed by the Commission whether the request contains objective, detailed and new reasons that have arisen since the designation decision. Providers may request reassessment at the earliest six months after the designation decision.
All general-purpose AI models with systemic risk are contained in a list published and up to date, without prejudice to the need to observe and protect intellectual property rights and confidential business information or trade secrets in accordance with EU and national law. The information to share to the Commission shall include the technical documentation of the model, including its training and testing process and the results of its evaluation that should be up-to-date, constantly integrated and enable a good understanding of the capabilities and limitations. The information regarding also training and testing processes. In fact, the providers of general-purpose AI models with systemic risk shall:

- Perform model evaluation in accordance with standardised protocols and tools reflecting the state-of-the-art, including conducting and documenting adversarial testing of the model with a view to identifying and mitigating systemic risk;
- Assess and mitigate possible systemic risks and

track their sources enabling identification of their origin;

- Keep track of document and report relevant information about serious incidents and possible corrective measures to address them;
- Ensure an adequate level of cybersecurity protection for the general-purpose AI model with systemic risk and the physical infrastructure of the model.

Providers of general-purpose AI models with systemic risk may rely on codes of practice to demonstrate that their compliance with the European harmonised standard; those who do not adhere to the approved code of practice shall demonstrate it with alternative adequate for achieve the approval by the Commission. The codes of practice shall include the following issues:

- To ensure that the information is kept up to date in the light of market and technological developments;
- An adequate level of detail for the summary about the content used for training;
- The identification of the type, the nature, and the sources of the systemic risks at EU level;
- The measures, procedures and modalities for the assessment and management of the systemic risks, taking into account their severity and probability of those risks may emerge and materialise along the AI value chain.

The **AI Office and the Board** shall aim to ensure that the codes of practice clearly set out their specific objectives and contain commitments or measures to ensure the achievement of those objectives considering the needs and the interests of all interested parties at European Union level.

Innovation

To encourage and facilitate the development of innovative AI technologies, it must be developed within a secure, compliant, and ethically grounded framework. To achieve this, the AI Act provides for the establishment of regulatory sandboxes for AI, tailored support measures for SMEs, including startups, and also includes specific exemptions for microenterprises. These measures enable the strengthening of the AI ecosystem while ensuring adherence to Regulation standards.
Regarding regulatory sandboxes, these refer to a controlled environment where supervised intermediaries and FinTech industry operators can test, for a limited period, technologically innovative products and services in the banking, financial, and insurance sectors[3]. The concept of regulatory sandboxes for AI is introduced as a controlled environment that fosters innovation by allowing the development, training, testing, and validation of AI systems under the supervision and guidance of competent authorities. Member States are required to establish at least one national **AI regulatory sandbox**, which could also be set up in collaboration with other Member States. Additionally, it is envisaged that additional regulatory AI sandboxes may be established at the regional or local level.
The establishment of regulatory AI sandboxes aims to pursue the following objectives:

- Improve legal certainty to achieve regulatory compliance with the AI Act or other applicable EU and national laws;
- Support the sharing of best practices through cooperation with the authorities involved in the regulatory sandbox;
- Promote innovation and competitiveness and facilitate the development of an AI ecosystem;
- Contribute to evidence-based regulatory learning;
- Facilitate access to the EU market for AI systems, particularly when provided by SMEs, including startups.

According to the AI Act, national authorities must ensure the participation of data protection authorities and other authorities involved in the processing of personal data in the operation of regulatory sandboxes for AI. Providers in the sandbox remain liable for damages caused but will not be fined if they comply with directives and conditions. Additionally, regulatory AI sandboxes must be designed and implemented to facilitate cross-border cooperation among national competent authorities. Such authorities must submit annual reports to the AI Office and the Council, starting one year after the establishment of the sandbox and every subsequent year until its cessation, and a final report providing information on the progress and results of the implementation of such sandboxes.
In order to prevent fragmentation of regulatory AI sandboxes within the EU, the Commission can adopt implementing acts specifying detailed provisions for the creation, development, implementation, operation, and supervision. These implementing acts include common principles on issues, such as:

- Eligibility and selection criteria for participation in regulatory AI sandboxes;
- Procedures for application, participation, monitoring, exit, and termination of regulatory AI sandboxes, including sandbox plan and exit report;
- Terms and conditions applicable to participants.

The above-mentioned acts will ensure that regulatory AI sandboxes are accessible to any potential provider of an AI system that meets transparent and fair eligibility and selection criteria, and will also ensure broad and fair access, taking into account the demand for participation. Access to the sandboxes are free for SMEs, including startups, and potential providers will be facilitated through the learning outcomes of the sandboxes in fulfilling compliance assessment obligations required by law. Furthermore, the sandboxes facilitate the involvement of other actors in the AI ecosystem, enabling and facilitating cooperation with both the public and private sectors.
The AI Act provides that personal data collected legally for other purposes may be processed within a regulatory sandbox to develop, train, and test specific AI systems. The processed data must be necessary to comply with specific regulatory requirements. Personal data must be kept in a separate and secure environment under the provider's control. The processing of personal data must not affect the decisions or rights of data subjects, and appropriate measures must be taken to protect data and ensure privacy. AI systems must be developed to safeguard a substantial public interest by a public authority in areas such as public safety, healthcare, environmental protection, energy sustainability, transportation security, and public administration efficiency.

Testing of High-Risk AI System in Real World Conditions Outside AI Regulatory Sandboxes

High-risk AI systems may undergo testing outside of regulatory sandboxes. Testing of high-risk AI systems in real-world environments outside of defined regulatory areas for AI may be conducted by providers or potential providers of such systems listed in a reference document, following a set of specific guidelines and procedures. These guidelines include preparing a detailed testing plan, obtaining

approval from a competent authority, and ensuring the protection of individuals involved in the test. Before participating in such tests, obtaining informed consent from the individuals involved is necessary. These individuals must be fully informed about the nature and objectives of the test, the methods used, the expected duration, as well as their rights during the test, including the right to withdraw without consequences. They must also be informed about how they can request modifications or reject decisions made by the AI system. Lastly, it is important that consent is documented, and a copy is provided to the participants or their legal representatives.
Furthermore, the AI Act establishes specific measures that suppliers and users, especially SMEs and startups, must adhere to. Indeed, Member States are required to actively support SMEs and startups within the framework of AI regulation, ensuring their priority access to regulatory AI sandboxes while respecting established requirements. Additionally, Member States must organize awareness and training activities tailored to the needs of these companies, involving local public authorities if necessary, and maintain dedicated communication channels and promote SME participation in standard development.
Meanwhile, the AI Office plays a key role in ensuring regulatory compliance by providing standardized templates, informative platforms, and promoting best practices in the procurement processes of AI systems. Microenterprises may comply with certain elements of the required quality management system in a simplified manner, provided they do not have partners or linked enterprises that would disqualify them from such simplifications. To this end, the AI Act stipulates that guidelines will be developed to assist these microenterprises in understanding and implementing these simplified compliance measures.

Governances

The **European Artificial Intelligence Board** is hereby established and represents a significant initiative aimed at fostering closer collaboration among the Member States in the field of AI. This body will consist of one representative from each member country, with the European Data Protection Supervisor participating as an observer. Despite lacking voting rights, the AI Office attends Council discussions. Operational procedures of the Council are outlined, with its presidency assigned to one of the representatives from the Member States, while the AI Office handle meeting organization and provide necessary administrative support. Member countries select their representatives for a three-year term, with the option for renewal once. These representatives must possess the necessary expertise to effectively carry out the tasks assigned by the Council.
The AI Office aims to ensure that the Council can carry out its activities effectively and impartially, promoting adequate governance in the AI sector. The Council, on the other hand, consult and assist the Commission and the Member States to ensure consistent application of the AI Act and it assists national authorities and the Commission in skill development, provides guidance on drafting guidance documents, and offers opinions on international AI-related matters and qualified alerts regarding general-purpose AI models. Among its functions, the Council coordinates the involved national authorities, shares knowledge and best practices, provides guidance on AI Act implementation, harmonizes administrative practices, issues recommendations on various matters, supports the promotion of AI literacy, and contributes to effective international cooperation. Finally, it considers the opinions of the Member States on the implementation of the regulation and the monitoring of AI systems.
Furthermore, there is a consultative forum that provides technical expertise and advice to the Council and the Commission, thereby supporting their tasks under this regulation. This consultative forum is composed in a diverse and balanced manner, including representatives from industry, start-ups, SMEs, civil society, and academia. selected by the Commission from among those with recognized expertise in the field of AI. Members will serve a two-year term, extendable up to four years. From certain organizations such as the Fundamental Rights Agency, ENISA, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI) the members shall be permanent. Member States may engage experts from the scientific panel to support their implementation activities of the regulation, potentially subject to fees. To this end, the Commission takes care of facilitating the access of such experts, which must occur promptly, and will ensure efficient organization of the support provided by both the experts and the European Union's AI support, aiming to maximize added value. Additionally, Member States may request assistance from experts of the scientific panel to implement the regulation. They may be subject to fees for the support received, which will be determined in the implementing act taking into account the regulation's objectives, cost-effectiveness, and fair access to experts.
Each Member State is required to establish or designate notifying authorities and market surveillance authorities for the purposes of the regulation. These authorities must act independently, impartially, and without bias, and must be equipped with adequate resources and expertise in AI technologies and related fields. Member States must also designate a single point of contact for the regulation and submit a report to the Commission every two years on the resources and adequacy of national competent authorities. Additionally, they may engage experts from the scientific panel to support their enforcement activities under the regulation, whose access is facilitated by the Commission, ensuring efficient organization of support activities. Furthermore, these experts can provide assistance for the implementation of the regulation and may charge fees, which will be determined in the implementing act, for the support provided to the Member States. These authorities must act independently, impartially, and without bias, equipped with adequate resources and expertise in AI technologies and related fields. Member States must also designate a single point of contact for the regulation and submit a biennial report to the Commission on the resources and adequacy of national competent authorities.

EU Database for High-Risk AI System

The database serves as a critical component of the EU's regulatory framework for AI, designed to enhance transparency, accountability, and oversight of high-risk AI systems. The European Commission, in collaboration with Member States, is tasked with setting up and maintaining a properly **EU database** with functional specifications determined in consultation with relevant experts and the **European Artificial Intelligence Board** for updates, ensuring that it meets the evolving needs of regulatory oversight.
The database is designed to include specific information sets which providers or their authorized representatives must enter. This structured approach ensures comprehensive documentation of high-risk AI systems, including their development, deployment, and compliance status. The information contained in the database shall be accessible and publicly available in a user-friendly manner easily navigable and machine-readable.

Nevertheless, there is information available exclusively to market surveillance authorities and the Commission unless consent for public access is provided by the provider or prospective provider. This tiered access safeguards sensitive information while promoting transparency where appropriate. The inclusion of personal data in the database is limited to what is necessary for fulfilling the Regulation's objectives, focusing on the names and contact details of individuals responsible for system registration with legal authority to represent providers or deployers. This measure balances the need for accountability with privacy and data protection principles.
The Commission acts as the controller of the EU database, providing technical and administrative support to providers, prospective providers, and deployers to facilitate compliance. The database's design and operation adhere to applicable accessibility requirements, ensuring it is user-friendly and accessible to all stakeholders. Through careful management of personal data and a commitment to accessibility, the EU database embodies the Regulation's principles of transparency, accountability, and privacy.

Post-Marketing Monitoring, Information Sharing, Market Surveillance

Post-Market Monitoring

Providers are mandated to establish a post-market monitoring system, which is proportional to the AI technology's nature and associated risks. This system should actively collect, document, and analyze relevant data to evaluate the AI systems' ongoing compliance with requested requirements. The data can come from deployers or other sources and must include performance metrics across the AI systems' lifecycle. A post-market monitoring plan, part of the technical documentation, guides this process. The Commission is tasked with developing a template for this plan, ensuring consistency and thoroughness in monitoring practices.

Sharing of Information on Serious Incidents

Providers of high-risk AI systems placed on the EU market shall report any serious incident to the market surveillance authorities of the Member States where that incident occurred. The timeframe for reporting depends on the incident's severity, with a general guideline of no later than 15 days after recognizing a causal link between the AI system and the incident. For particularly grave incidents, such as those leading to death, reports must be made within two days. Providers are required to investigate serious incidents promptly and cooperate with competent authorities, ensuring that any necessary corrective action is taken. National competent authorities shall immediately notify the Commission of any serious incident, whether they have acted on it.

Enforcement

Under Regulation (EU) 2019/1020[15], the AI Regulation shall be aligned with the broader framework of market surveillance, defining the scope of market surveillance activities, and clarifying the roles of various national authorities in overseeing high-risk AI systems. The procedures shall not apply to AI systems when exist already relevant sectoral procedures ensuring an equivalent level of protection and having the same objective. Guaranteeing full access to the documentation and the training, as well as validation and testing data set used for the development of high-risk AI systems (i.e., application programming interfaces ("API")) or other relevant technical means and tools enabling remote access to have as purpose to ensure the compliance with the Regulation. This includes overseeing testing within AI regulatory sandboxes and verifying adherence conditions. Authorities have the power to modify, suspend, or terminate testing if necessary to protect public safety and compliance with the regulation.
Respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect both the intellectual property rights, confidential business information or trade secrets of a natural or legal person. Put in place adequate and effective cybersecurity measures and shall delete the data collected as soon as it is no longer needed for the purpose for which it was obtained, in accordance with applicable EU or national law.

Remedies

For to allow any individual or entity to submit complaints to authorities if they believe there has been a breach of the Regulation's provisions, are available two remedies toward high-risk AI systems, more specifically:

- **Right to Lodge** a Complaint with a Market Surveillance Authority when it is believed there has been a breach of the Regulation's provisions: such complaints shall be taken into account for the purpose of conducting market surveillance activities and shall be handled in line with the dedicated procedures established therefor by the market surveillance authorities.
- **Right to Explanation** of Individual Decision-making; it allows to affected persons have the right to obtain clear and meaningful explanations from deployers about the role and impact of high-risk AI systems in individual decision-making processes, especially when these decisions significantly affect their rights, health, or safety.

Supervision, Investigation, Enforcement and Monitoring in Respect of Providers of General-purpose AI Models

The Commission has the power to supervise and enforce and, for the implementation of these tasks, shall entrust the activity to the AI Office which may take the necessary actions to monitor the effective implementation and compliance with the Regulation by providers of general-purpose AI models, including their adherence to approved codes of practice. The market surveillance authorities may request the Commission to exercise specific powers when and proportionally to assist with the fulfilment of their tasks.
Providers shall have the right to lodge a complaint alleging an infringement of the Regulation and, when the alerts come from the scientific panel, defined qualified alert, is the Commission that assesses the matter. For both above situations, the Commission may request the provider of the general-purpose AI model concerned to provide the documentation drawn up and any additional information that is necessary for the purpose of assessing compliance of the provider or the general-purpose AI model.
These actions are critical in ensuring the ongoing compliance of AI systems with the Regulation's standards, safeguarding public safety, and protecting fundamental rights.

Codes of Conduct and Guidelines

Regarding the role and formulation of codes of conduct and guidelines, their aim is to promote the voluntary appli-

cation of specific requirements to AI systems beyond those classified as high-risk.
Referring the **codes of conduct**, the AI Act establishes that the AI Office, alongside Member States, have the task of encouraging and facilitating their creation. These codes, aiming to broaden the scope of requirements to encompass AI systems not classified as high-risk, are designed to incorporate industry-specific technical solutions and best practices. This initiative reflects a wider aspiration to promote the ethical development of AI beyond the confines of regulatory mandates. The AI Office and Member States are tasked with fostering the creation of voluntary codes for the use of AI systems, characterized by specific requirements aligned with clear objectives and measurable performance indicators, including EU ethical guidelines, environmental impact assessment and mitigation, promotion of AI literacy, inclusive system design, and prevention of adverse effects on vulnerable groups, including individuals with disabilities, and promotion of gender equality. Additionally, such codes may be developed by individual providers or users, their representative organizations, or through collaborative efforts involving stakeholders from civil society and academia. As for their intended purposes, these are developed to address the unique needs and challenges encountered by SMEs, including startups. This enables smaller entities to readily adopt and adhere to elevated ethical standards and practices, thereby promoting widespread commitment to responsible AI across the ecosystem.
Regarding **guidelines**, the Commission is responsible for drafting guidelines to facilitate the practical implementation of the Regulation, covering a wide range of areas from the application of specific requirements and obligations to the management of prohibited practices and transparency obligations. These guidelines are designed to clarify and facilitate compliance, ensuring that stakeholders across the AI landscape can effectively navigate the regulatory framework. The Commission, according to AI Act, has produced guidelines for the practical implementation of the AI Regulation. In drafting these guidelines, the Commission must consider the specific needs of SMEs, including startups, local public authorities, sectors most likely to be influenced by the Regulation, and additionally, the state of the art in AI, relevant harmonized standards and common specifications, as well as provisions on EU harmonization. Recognizing the rapid evolution of AI technology and its applications, the Commission is tasked with updating these guidelines as necessary, whether at the request of Member States, the AI Office, or on its own initiative. This adaptive approach ensures that the guidance provided remains relevant and responsive to technological advancements and emerging best practices in the field.

Delegation of Power and Committee Procedure

The AI Act regulates delegated acts, outlining the procedural aspects related to the committee assisting the Commission.

Delegated Acts

The European Commission is empowered to adopt delegated acts, allowing it to amend non-essential elements of the Regulation or integrate it, subject to the procedures outlined in this chapter.
The delegation of powers is initially granted for a period of five years from the entry into force of the Regulation, with automatic renewal for identical periods unless there is explicit opposition from the European Parliament or the Council.
The Commission also has the power to adopt specific delegated acts in various articles for a period of five years from the date of entry into force of the regulation. Additionally, it must submit a report on the delegation of powers no later than nine months before the end of the five-year period. The renewal of the delegation will be automatic unless the European Parliament or the Council oppose it within three months before the end of each period. The delegation of powers outlined in the AI Act can be revoked by the European Parliament or the Council at any time and will take effect from the day following its publication in the Official Journal of the European Union.
Before adopting a delegated act, the Commission is required to consult experts designated by each Member State, respecting the principles of best legislation, and ensures that delegated acts reflect the experience and perspectives of the Member States, promoting a collaborative approach to regulation. After adopting a delegated act, the Commission must notify both the European Parliament and the Council simultaneously, maintaining a transparent and inclusive legislative process.

Committee Procedure

The committee provides its opinion on acts that must be adopted on the proposal of the Commission:

- If the committee expresses a positive opinion, the Commission adopts the draft implementing act;
- If the committee expresses a negative opinion, the Commission does not adopt the draft implementing act. However, the President of the Commission can submit a modified version to the committee within a month or to the appeal committee for a new decision;
- If no opinion is expressed, the Commission adopts the draft implementing act. If the Commission does not adopt the draft implementing act, the President can submit a modified version to the committee.

The Commission does not adopt the draft implementing act if it concerns certain sectors (taxation, financial services, protection of human, animal, or plant health or safety, multilateral definitive safeguard measures), if the basic act provides for it, or if a simple majority of the committee members opposes it. The president may submit a modified version to the same committee within two months or to the appeal committee within one month for a new deliberation, based on the aforementioned cases of non-adoption. The Commission consults with the Member States and informs the committee of the results. The appeal committee convenes to provide its opinion on the draft implementing act.

Penalties

The AI Act outlines the framework for imposing **sanctions** on operators who violate the provisions established therein. These aim to enforce the provisions of the AI Act and ensure compliance, thus protecting the public interest, fundamental rights, and safety standards in the context of AI development and implementation.
In accordance with the AI Regulation, Member States must establish sanction rules and implement enforcement measures for operator violations. These rules may include **warnings** and **non-monetary measures** and must be effectively implemented, taking into account the Commission's guidelines. Sanctions must be effective, proportionate, and dissuasive, also considering the interests of SMEs and startups. Member States must notify the Commission of the

sanction rules and other enforcement measures, promptly informing it of any subsequent changes. Operators that do not comply with the prohibition of certain AI practices (see chapter "Prohibited AI practices") are subject to **administrative fines** of up to €35 million or up to 7% of the total worldwide annual turnover for the preceding financial year, whichever is higher. Additionally, non-compliance with obligations related to providers, authorized representatives, importers, distributors, deployers, notified bodies, and transparency obligations can result in fines of up to €15 million or up to 3% of the total worldwide annual turnover for the preceding financial year, whichever is higher. Providing incorrect, incomplete, or misleading information to notified bodies or national competent authorities in response to a request is subject to administrative fines of up to €7.500.000 or up to 1% of the company's total worldwide annual turnover for the preceding financial year, whichever is higher. For SMEs, including startups, each fine is capped at lower percentages or amounts as specified in the Regulation, ensuring penalties do not disproportionately impact smaller businesses.
When assessing the imposition and quantification of an administrative sanction in a specific case, it is essential to consider all relevant factors of the situation. These include the nature, gravity, and duration of the infringement and its consequences, taking into account the purpose of the AI system and the extent of people's involvement and the damages incurred. It is also important to ascertain whether other market surveillance authorities have already penalized the same operator for the same violation or if sanctions have been imposed for breaches of other laws, in addition to evaluating the size, annual turnover, and market share of the operator. Other significant factors include the financial benefits gained or losses avoided as a result of the infringement, the level of cooperation with authorities to resolve the violation, the degree of responsibility, and the actions taken by the operator to mitigate the harm suffered by those involved. Furthermore, it is crucial to determine whether the infringement was intentional or due to negligence.
Member States are tasked with establishing rules on how administrative fines may be imposed on public authorities and bodies within their jurisdiction. Depending on the legal system of the Member States, the provisions regarding administrative sanctions can be implemented in various ways: penalties may be imposed by competent national courts or by other bodies, in accordance with national laws. However, the application of such provisions must ensure an equivalent effect across all relevant Member States. The market surveillance authority, in exercising its powers, must adhere to appropriate procedural safeguards in line with both EU and national law, ensuring the possibility of effective judicial remedies and adherence to the principle of due process. Finally, on an annual basis, Member States must report to the Commission the administrative fines issued during that year, as well as any related legal or judicial proceedings.

Entry into Force and Review

Regarding AI systems that have already been placed on the market or put into service before certain deadlines specified in the Act, AI Act outlines a timeline for bringing these systems into compliance with the Act's requirements, providing a transition period for operators to adjust to the new regulatory environment. The AI Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It shall apply from 24 months from the date of entry into force of this Regulation. However:

- Provisions regarding **Prohibited** AI system shall apply from **6 months** from the date of entry into force of this Regulation (mid-December 2024);
- Provisions and rules regarding **General Purpose AI** shall apply from **12 months** from the date of entry into force of this Regulation (mid-July 2025);
- Provisions and rules regarding **High risk AI system** shall apply from **24 months** from the date of entry into force of this Regulation (mid-July 2026);
- Provisions and rules regarding for **AI related to Harmonized Products** shall apply from **36 months** from the date of entry into force of this Regulation (mid-July 2027).

This provision reflects the Act's forward-looking approach while acknowledging the need for a gradual transition for existing AI systems.
The Commission is tasked with regularly evaluating and reviewing the Act to assess the need for amendments, including updates to the list of high-risk AI systems and prohibited AI practices (by four years from the date of entry into force of this Regulation and every four years thereafter). The evaluation process will consider the Act's impact on market entry for new undertakings, particularly SMEs, the adequacy of resources for national competent authorities, the application of penalties, and the development of harmonized standards. This ongoing evaluation ensures that the Act remains relevant and effective in the face of technological advancements and market developments. The AI Office is expected to develop a methodology for evaluating risk levels and including new systems in the lists of high-risk AI systems, prohibited practices, and systems requiring additional transparency measures. This support is crucial for maintaining a dynamic and responsive regulatory approach to AI.
The Regulation will enter into force on the twentieth day following its publication in the Official Journal of the European Union and will be applicable from 24 months after its entry into force. However, certain chapters and provisions have different application timelines to ensure a phased implementation of the Act; (i) Provision regarding prohibited AI system shall apply from six months from the date of entry into force of this Regulation and (ii) other provision regarding high-risk AI system shall apply from 12 months from the date of entry into force of this Regulation. This staged approach facilitates a smooth transition for stakeholders to adapt to the new regulatory requirements.

AI Regulation in Other Countries and the Actions

Regarding other **extra-Europe countries**[19][26], on October 30th 2023, **Unites States** President Biden signed an *"Executive Order (EO) on Safe, Secure, and Trustworthy Artificial Intelligence"*[28]. This EO builds on previously published guidance documents such as the AI *"Bill of Rights"*[27] and the National Institute for Standards in Technology (NIST) AI Risk Management Framework[22]. The order defines AI broadly and lays out eight principles and priorities for the use of AI:

- AI must be safe and secure;
- The US should promote responsible innovation, competition and collaboration in AI development;
- The responsible use and development of AI must come with a commitment to supporting American workers;

- AI policies must be consistent with the Biden Administration's dedication to improving equity and civil rights;
- Interests of Americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives must be protected;
- Americans' privacy and civil liberties must be protected;
- The risks from the Federal Government's own use of AI must be adequately managed and the government's capacity to;
- The US Federal Government should lead the way and engage with international partners to develop a framework to manage AI risks and unlock potentials.

China has implemented interim measures to address AI-related risks and impose compliance obligations on entities engaged in AI-related business. Provisions only apply to public usages of gen-AI[4] by both domestic and foreign individuals and entities involved in AI services in China. A draft version of the interim measures was released for comments in April 2023[6], followed by a substantially revised version dated July 2023 [5] and taking effect on August 2023. Similar to the EU AI Act, the measures do not apply to gen-AI technologies used for research purposes and not deployed to the market. Encouragement for gen-AI development was also added. Key points of the July 2023 *"Interim Measures for the Management of Generative Artificial Intelligence Services"* are:

- Gen-AI services providers with public opinion properties or with the capacity for social mobilization shall carry out security assessments in accordance with relevant state provisions.
- Obligors must comply with laws, social morality, and ethics, and avoid manipulating information or public opinion. During algorithm design, selection of data, model generation and training, and provision of services, effective measures should be employed to prevent biases that result in discrimination. Providers shall fulfill confidentiality obligations towards information input by users and users' usage records in accordance with existing laws.
- Content is prohibited if it is against *"Core Socialist Values"* or if it otherwise endangers national security. Providers are responsible for the legality of content generated and diffused, and for prompt interruption of services and rectification of unlawful content.
- Intellectual property rights should be protected and advantages in algorithms, data, platform and the like must not be used for monopolies or to carry out unfair competition.
- Penalties for non-compliance include warnings, ordering rectifications and corrections, suspension of services, as well as civil and criminal prosecution when relevant.

In the **UK**, several authorities are involved in the regulation of AI, and the regulatory approach is characterized by guidelines, best practices and principles. Examples of key initiatives include *"Defence Artificial Intelligence Strategy"*[20], *"Guidance on AI and Data Protection"*[29] and the UK's NCSC's *"Guidelines for Secure AI System Development"*[21]. In March 2023, the UK Government issued a white paper for *"A Pro-Innovation Approach to AI Regulation"*[25]. This paper stresses a regulatory attitude based on specific areas of application of AI rather than specific technologies. It suggests that potential future regulation shall focus on principles such as safety, transparency, fairness, accountability, and contestability. The paper excludes immediate regulatory action, delineating instead plans to invest in AI research and development, and to collaborate with international partners to influence global AI governance. The UK Government is currently working on a *"Code of Practice"* on Copyright Issues and AI[18].

AI's impacts have a global component that calls for international cooperation. In addition to strategic considerations, the need for cooperation emerges from externalities inherent to the technology that may spill over national borders, or regulation themselves. The cooperation may be complicated by contrasting objectives and definitions of social welfare. Below it is reported some initiatives relative to international cooperation and multilateral actions relative to AI[19]:

- **OECD "AI Principles"**[24] - In May 2019, the OECD adopted a set of *"AI Principles"* to foster innovative and trustworthy AI that respects human rights and democratic values. The five principles are: i) inclusive growth, sustainable development and well-being, ii) human-centered values and fairness, iii) transparency and explainability, iv) robustness, security and safety, and v) accountability. The principles have since been endorsed by 46 countries worldwide and have been embedded in several national and multinational initiatives.
- **NATO AI strategy** - In its October 2021 meeting, the NATO Allied Defence Ministers formally adopted an AI strategy for defense and national security, committing to the cooperation and collaboration necessary for its implementation. Signatories committed to *"Principles of Responsible Use"*[23] for the development and deployment of AI. The six principles are: (i) Lawfulness; (ii) Responsibility and Accountability; (iii) Explainability and Traceability; (iv) Reliability; (v) Governability; and (vi) Bias Mitigation.
- **World Economic Forum** - In June 2023, The World Economic Forum (WEF) launched the *"AI Governance Alliance"*[31] to unite industry leaders, governments, academic institutions and civil society organizations around the goal of meaningful AI governance. Ultimately, AI's opportunities and challenges, including governance and regulation, were at the center of the 2024 Davos meetings.
- **UN initiatives** - In December 2023, The UN AI Advisory Body released the Interim Report *"Governing AI for Humanity"*[30]. The document calls for a closer alignment between international norms and AI's developed and deployment. The AI Advisory Body recommends five guiding principles: i) AI should be governed inclusively, by and for the benefit of all; ii) AI must be governed in the public interest; iii) AI governance should be built in step with data governance and the promotion of data commons; iv). AI governance must be universal, networked and rooted in adaptive multi-stakeholder collaboration; v). AI governance should be anchored in the UN Charter, International Human Rights Law, and other agreed international commitments such as the Sustainable Development Goals.

[4]Generative artificial intelligence (gen-AI) is artificial intelligence capable of generating text, images, videos, or other data using generative models, often in response to prompts. Generative AI models learn the patterns and structure of their input training data and then generate new data that has similar characteristics.

- **G7: "Hiroshima Process International Code of Conduct for Advanced AI Systems"** - On October 30, 2023, G7 leaders agreed to the *"Hiroshima Process International Code of Conduct for Advanced AI Systems"*. The code provides *"voluntary guidance for actions by organizations developing the most advanced AI systems"*[17]. The document lays out guidance principles encouraging: i) risk mitigation in all parts of the AI process; ii) increased transparency during development reporting systems' capabilities and domains of use; iii) sharing of information and reporting of incidents in development; iv) developing governance, v) increasing security controls and advance the development of international standards; vi) deploying reliable provenance mechanisms such as watermarking; vii) prioritizing research to increase AI's safety and on applications that would help sustainable development goals; viii) implementing data input measures and protection for personal data and intellectual property.
- **The first global "AI Safety Summit"** - On November 1-2, 2023 the British government hosted the first global *"AI Safety Summit"*, gathered representatives from 28 national governments. The initiative discussed how to approach and regulate AI technologies. On this occasion, the participating national governments and the EU signed the *"Bletchley Declaration"*[1], resolving to further national, multilateral and bilateral action to promote on AI safety research and establish risk-based policy across the respective countries.
- **Guidelines for Secure AI System Development** - In November 2023, the UK National Cyber Security Centre (NCSC), the US Cybersecurity and Infrastructure Security Agency (CISA), and several other national cyber security agencies across AEs and EMDEs released a set of Guidelines[21]. These guidelines aim to: a secure design, secure development, secure deployment, and secure operation and maintenance. The report includes suggestions about mitigations to related risks in the view that providers of AI components should take responsibility for the security outcomes of users further down the supply chain.
- **The Global Partnership on AI and the Ministerial Declaration** - The goal of the Global Partnership on AI is to guide the responsible development and use of AI. On occasion of the December 2023 general purpose AI summit in Delhi, Ministers of the 29 member countries signed a joint declaration reaffirming their commitment to promote responsible and trustworthy AI, and their dedication to jointly develop regulations, policies, and standards to uphold general-purpose AI's principles[16]. The Ministers also embraced the notion of *"collaborative AI"*, which involves supporting and promoting equitable access to critical resources for AI research and innovation, such as AI computing, high-quality diverse datasets, algorithms, software.

Final Provisions

The evolution of AI has been marked by rapid advancements in technology that have fundamentally transformed various sectors, including healthcare, transportation, finance, and more. Globally, AI's growth has prompted significant economic, social, and ethical implications. In the European Union, the implications of AI's evolution have been met with a proactive approach aimed at harnessing its benefits while addressing potential risks. The EU has recognized the need for a regulatory framework that ensures AI's development and use align with core values and fundamental rights, such as privacy, dignity, equality, and non-discrimination. The AI Act aims to establish harmonized rules for the development, marketing, and use of AI systems within the European Union. It focuses on ensuring AI systems are human-centric, trustworthy, and uphold fundamental rights, including privacy, non-discrimination, and consumer protection. Overall, the objectives of the AI Act reflect the European Union's ambition to lead in the development of ethical, secure, and cutting-edge AI technologies. The Act's successful implementation will require ongoing dialogue between regulators, industry stakeholders, and society to adapt to the evolving landscape of AI technologies.
While the Act aims to protect citizens' rights and safety, it also seeks to foster innovation and competitiveness in the AI sector, thanks to a continuous balance between regulation and encouragement of technological development, ensuring the EU remains a global leader in trustworthy AI.
However AI Act faces several challenges, these concerns primarily revolve around balancing innovation with regulation, addressing practical challenges in classification and compliance, and understanding the potential impacts on small and medium-sized enterprises (SMEs).

- One of the critical challenges of the AI Act is ensuring that the regulatory framework supports and does not stifle innovation.
- The Act's risk-based approach to AI regulation necessitates the classification of AI systems according to the level of risk they pose. This classification process could be complex and subject to interpretation, raising concerns about consistency and clarity in its application. Moreover, the requirement for high-risk AI systems to comply with stringent regulations poses practical challenges for developers and deployers in terms of technical documentation, data governance, and ensuring human oversight.
- SMEs play a crucial role in the EU's economy and are often at the forefront of innovation in AI. However, the regulatory obligations imposed by the AI Act could disproportionately affect these smaller entities. The costs associated with ensuring compliance, such as conducting risk assessments, maintaining extensive documentation, and implementing data governance and human oversight mechanisms, could be particularly challenging for SMEs with limited resources, hindering their ability to compete with larger companies and stifling innovation within the sector.

In response to these challenges and criticisms, ongoing dialogue between policymakers, industry stakeholders, researchers, and civil society is crucial. This dialogue can help refine the regulatory approach to ensure it remains effective, proportionate, and conducive to innovation. Moreover, the dynamic nature of AI technology necessitates regulatory frameworks that are flexible and adaptable, allowing for updates and revisions as the technology and its applications evolve. Given the global nature of AI development and deployment, international cooperation is crucial for establishing consistent standards and practices for AI governance. Collaborative efforts can help address cross-border challenges, such as data privacy, security, and the ethical use of AI technologies. The EU can play a leading role in fostering international dialogue, sharing best practices, and contributing to the development of global norms

for AI.
Furthermore, in the light of *Digital Operational Resilience Act* (DORA)[14] on the ICT sector, financial institutions should start to consider how DORA's imposed requirements interact with the obligations stemming from the AI Act. Indeed, DORA aims to ensure the ICT resilience of the EU financial sector and represents both a challenge and an opportunity to support, reboot and strengthen cyber resilience. The regulation addresses information security and ICT third party management for all regulated financial entities, introducing new requirements where gaps exist: (i) ICT risk management, (ii) ICT incident reporting, (iii) digital operational resilience, (iv) third-party ICT risk management and (v) information sharing agreements. Traditionally strong reliance of financial institutions on third-party ICT services will become even more prominent in the context of AI. Due to the lack of internal capabilities for the development of AI solutions, outsourcing to ICT service providers[7] is expected to increase, as will the security issues and challenges to the governance framework of institutions, particularly internal controls, data management and data protection.
Following the formal approval of the text of the AI Act, organizations and financial institutions can proactively begin preparing for compliance. The first step is to ensure the right people in the organization start preparing for these upcoming regulatory requirements as soon as possible. Early engagement give more time to understand the requirements and their impact across the AI lifecycle. The AI Act identifies various roles, including legal, privacy, data science, risk management and procurement professionals. A multidisciplinary task force responsible for compliance with the AI Act should cover this full range of expertise. The second step is to comprehensively understand AI systems developed or used in the organization and categorize them based on the risk levels defined in the AI Act, also with a proper inventory of this models. If any of AI systems fall into the minimal, high, or unacceptable risk category, you may be required to make significant changes to processes and operations before 2026 or sooner for AI systems with unacceptable risk. It is crucial to have a clear plan of what needs to be done as quickly as possible to manage the necessary organizational transformation and ensure timely compliance with the new legal framework when it comes into effect and transparency to stakeholders. When an AI system is not compliant with regulations, thorough gap analyzes should be conducted to identify areas of non-compliance and develop an action plan to address these gaps.
Regarding the financial institutions activities, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources. AI systems used for those purposes may lead to discrimination between persons or groups and may perpetuate historical patterns of discrimination, such as that based on racial or ethnic origins, gender, disabilities, age or sexual orientation, or may create new forms of discriminatory impacts. However, internal AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under this Regulation. Finally, AI systems intended to be used for risk assessment and pricing in relation to natural persons for health and life insurance can also have a significant impact on persons' livelihood and if not duly designed, developed and used, can infringe their fundamental rights and can lead to serious consequences for people's life and health, including financial exclusion and discrimination.

In conclusion, the AI Act represents a significant stride toward creating a harmonized and ethical framework for AI technologies. The Act's emphasis on fundamental rights and ethical considerations sets a global standard for AI governance, encouraging other regions to consider similar comprehensive and principled approaches. By balancing the promotion of innovation with the protection of individual rights, the EU aims to foster an AI ecosystem that is both dynamic and responsible. The AI Act is a landmark piece of legislation with far-reaching implications for the future of AI in the EU and beyond. It underscores the EU's commitment to leading the way in ethical AI governance, setting a benchmark for the world and ensuring that AI serves the public good while respecting human rights and democratic values.

References

[1] **AI Safety Summit.** *The Bletchley Declaration by Countries Attending the AI Safety Summit*. November 2023.

[2] **Banca d'Italia.** *Banking Insight 2023 - AI-driven bank: Opportunitá e sfide strategiche per il sistema finanziario e la vigilanza*. October 2023.

[3] **Banca d'Italia.** *Regulatory sandbox from Banca d'Italia Eurosistema*. April 2019.

[4] **Council of the European Union.** *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 - General approach*. November 2022.

[5] **Cyberspace Administration of China.** *China: Generative AI Measures Finalized*. July 2023.

[6] **Cyberspace Administration of China.** *Interim Measures for the Management of Generative Artificial Intelligence Services*. April 2023.

[7] **European Central Bank.** *ECB public consultation: Guide on outsourcing cloud services to cloud service providers (CSPs)*. June 2024.

[8] **European Commission.** *Ethics guidelines for trustworthy AI: High-Level Expert Group on AI*. April 2019.

[9] **European Commission.** *Proposal for a "Regulation od the European Parliament and of the Council: laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative acts"*. April 2021.

[10] **European Council.** *Artificial Intelligence Act: Council and Parliament strike a deal on the first rules for AI in the world*. December 2023.

[11] **European Council.** *Artificial Intelligence Act: Council gives final green light to the first worldwide rules on AI*. May 2024.

[12] **European Parliament.** *Artificial Intelligence Act*. June 2023.

[13] **European Parliament.** *Artificial Intelligence Act: MEPs adopt landmark law*. March 2024.

[14] **European Parliament.** *Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector*. December 2022.

[15] **Gazzetta Ufficiale dell'Unione Europea.** *Regolamento (UE) 2019/1020 del Parlamento Europeo e del COnsiglio del 20 giugno 2019 sulla vigilanza del mercato e sulla conformitá dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011*. June 2019.

[16] **Global Partnership on AI.** *GPAI Ministerial Declaration*. December 2023.

[17] **Group of Seven (G7) - Hiroshima.** *Hiroshima Process International Code of Conduct for Advanced AI Systems*. June 2023.

[18] **Intellectual Property Office.** *The government's code of practice on copyright and AI*. June 2023.

[19] **International Monetary Fund.** *The Economic Impacts and the Regulation of AI: A Review of the Academic Literature and Policy Actions*. March 2024.

[20] **Ministry of Defence.** *Defence Artificial Intelligence Strategy*. June 2022.

[21] **National Cyber Security Center.** *Guidelines for secure AI system development*. November 2023.

[22] **National Institute of Standards and Technology.** *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. January 2023.

[23] **North Atlantic Treaty Organization.** *An Artificial Intelligence Strategy for NATO*. October 2021.

[24] **Organisation for Economic Co-operation and Development.** *OECD AI Principles overview: Principles for trustworthy AI*. May 2019.

[25] **Parliament by the Secretary of State for Science, Innovation and Technology.** *A pro-innovation approach to AI regulation*. August 2023.

[26] **Standford University Human-Centered Artificial Intelligence.** *Artificial Intelligence Index Report 2024*. April 2020.

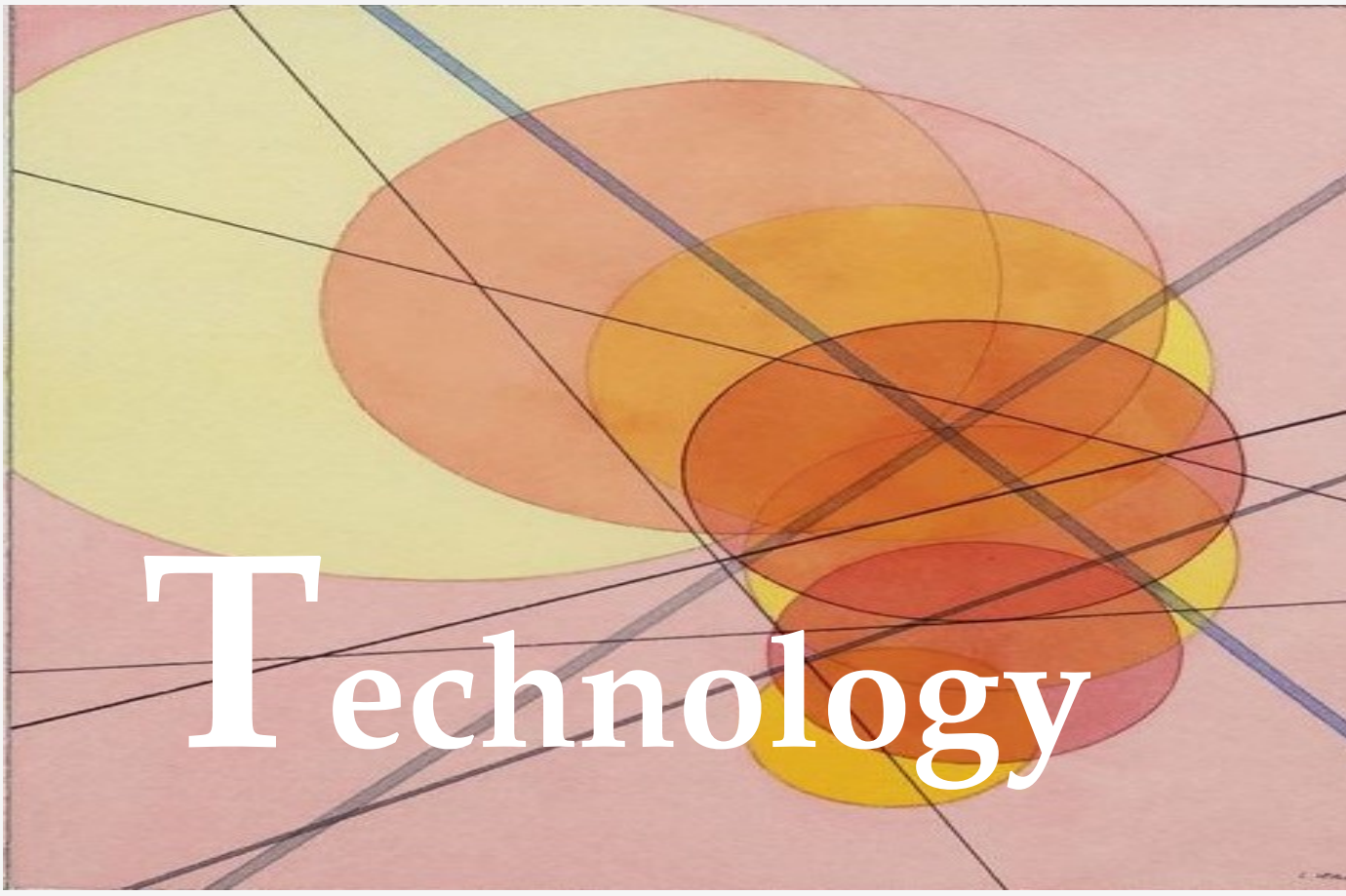
[27] **The White House.** *Blueprint for an AI Bill of Rights*. June 2022.

[28] **The White House.** *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. November 2023.

[29] **UK's Information Commissioner's Office.** *Guidance on AI and data protection*. March 2023.

[30] **United Nations.** *Interim Report: Governing AI for Humanity*. December 2023.

[31] **World Economic Forum.** *AI Governance Alliance*. June 2023.



Exploring the Digital Renminbi: Insights into Chinas CBDC

About the Authors

Gianmarco Mori:
Senior Financial Engineer
He holds a Bachelor in Banking and Finance and a Master degree in Statistics and Actuarial science. He obtained a specialization in Quantitative Finance at Politecnico di Milano and he had worked in a consulting firm for two year focused in Credit and Liquidity Risk Management. After these years, he moved to banking sector in Risk Management area and currently he has been working in Iason as financial engineer for some of the major italian players.

Mattia Bainotti:
Financial Engineer
He holds a MSc in Finance from Università del Piemonte Orientale paired with a postgraduate specialization degree in Quantitative Finance and Risk management from Università di Torino, Collegio Carlo Alberto.

Gaspare Campaniolo:
Project Manager
He holds a bachelor's in management engineering and a Master degree in Supply Chain Management at Politecnico di Milano. After the graduation, he began his career at Iason, where he has been working for about 1 year, involved in a project aimed at the development of the internal model for the insurance division of one of Italy's largest banks.

Gabriele Donadoni:
Business Analyst
He studied Mathematical Engineering at Politecnico di Milano specializing in Quantitative Finance. He is currently involved in a project aimed at the development of the Internal Model for the insurance division of one of Italy's largest banks

Fabrizio Gentalavigna:
Senior Business Analyst
Graduated in Business Administration from the university of Naples "Federico II". Joined to Iason in 2023 working on projects mainly focused on market risk. At the end of 2023 he worked in the inspection process on the sensitivity mismatch required by the ECB

Riccardo Greco:
Credit Risk Quant
He obtained an MSc in Statistical Sciences from the University of Bologna. He began his tenure with iason in May 2023 and, as a Credit Risk Analyst, he has been involved in developing credit risk models for major banking institutions.

Marco Zanolli:
Credit Risk Quant
With his MSc degree in Statistics he developed a deep knowledge of the mathematical theory behind most of the econometric models used in Finance. He is currently involved, as a Credit Risk Quant, on ICAAP and Stress Test exercises at one of the major Italian banks.

This document was prepared in collaboration with Pietro Maria Cepparulo and Nicola Mazzoni, who at the time were working for Iason Consulting.

Exploring the Digital Renminbi: Insights into Chinas CBDC

Gianmarco Mori
Pietro Maria Cepparulo
Riccardo Greco
Mattia Bainotti
Gabriele Donadoni
Nicola Mazzoni
Gaspare Campaniolo
Fabrizio Gentalavigna
Marco Zanolli

In an era where digital innovations intersect with technology and finance, profound shifts are catalyzing changes in traditional monetary systems. Within this evolving landscape, CBDCs are gaining momentum, and this paper aims to explore the distinctive features and potential applications of China's Digital Renminbi, beginning with a comprehensive overview of CBDC fundamentals and the evolution of the e-CNY development. Following this foundational overview, the paper will report an assessment of financial inclusion across China, contextualizing the role and impact of CBDCs. The core part of the paper will focus on the design of the architectural model, delving into its distribution model, the key principles underlying the Digital Wallets and the technological framework that supports the Chinese CBDC. The final section introduces the cross-border payment paradigma with mBRIDGE, a project at first and then a real exchange platform. The international involvement of the participants acted as a sounding board to raise awareness of the collaboration between central banks, commercial banks and corporate institutions. Considerations will be given regarding a future made of interconnections, where efficiency and privacy play a key role.

The financial sector has seen a period of important changes over the last few years due to improvements in technological innovation and changes in user preferences. In this scenario, considering the decline in cash usage and the increase in the development of digital payment platforms, Central Bank Digital Currencies have become a focal point in the field of central bank analysis for modernizing monetary systems without compromising central bank authority. In this sense, China's Digital Renminbi has led the world's major economies in pushing forward the development of the CBDC project with its advancements in the development of its CBDC, the Digital Renminbi. The purpose of this paper is to outline the progress in the Digital Renminbi development, describing its peculiarities by examining the architecture of e-CNY, its possible benefits, and its broader implications in the global landscape of CBDC development. More precisely, the analysis will cover the characteristics that identify the design of the Digital Renminbi, explaining the peculiarities of its two-tier distribution model, the e-CNY digital wallet typologies, and the technologies behind it. The conclusions will underline the cross-border implications of e-CNY and further outline the ongoing development status of the mBridge project. Considerations through this discussion will lead to studying the implications of a future made up of interconnections, where efficiency and privacy intervene as two key players.

Introduction to CBDC

The technological innovations of the last decade have brought disruptive changes in the financial sector. In particular, we have witnessed a shift in user behavior with a decline in cash usage in favor of new ways of payments and the rise of new platforms that offer diversified services related to financial services. In this context, Central Banks have begun to closely monitor these new paradigms with a certain concern about the possibility that central bank money (the money that is issued by a Central Bank and guaranteed by the public authority, in contrast with the commercial money that is the money detained at banks that are guaranteed by the financial stability of a particular institute) will lose its importance as the center of the exchange system. These conditions are the ones that have fostered the increasing interest in the Central Bank Digital Currencies (CBDC). CBDCs are nothing less than fiat money issued at par with the physical money issued by the Central Bank that will serve as a payment method, being so legal tender money, and a store of value such as its paper counterpart. CBDC could also be distinguished by the plethora of users that they are designed for: wholesale CBDCs are distributed among financial institutions and used for interbank transactions, while retail CBDCs are intended for the general public, retail users, and businesses. This chapter aims to clarify the main features that a Central Bank could take into consideration while planning to issue a CBDC and also inquiring the potential benefits and implications for the financial sector and the political economy.

The CBDC Environment

Distribution Models

In the development of the CDBC system, one of the most important decisions to be taken into consideration is the role that actors of the economic system have to fulfill in terms of issuing and distributing the CBDC. The design of the Distribution Model involves the duties that have to be covered regarding the management of:

- **CBDC Issuing;**
- **Transaction Management;**
- **Users Relationship.**

Three models are usually considered to address a CBDC system, and these can be distinguished as follows:

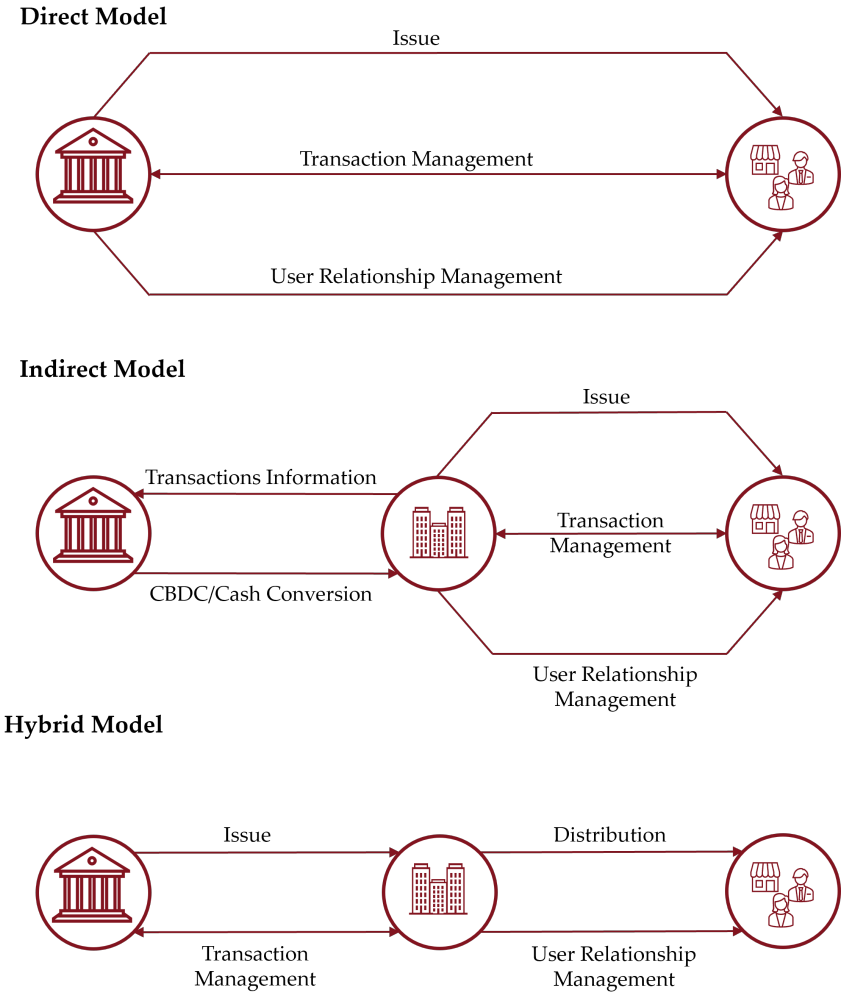


FIGURE 2: Distribution Models

- **Direct Model;**
- **Indirect Model;**
- **Hybrid Model.**

In the Direct Model, the Central Bank plays a pivotal role within the system considering that this configuration requires that all the activities regarding the issue, the transaction management, and the users'relationship must be performed by the Central Bank. The Direct Model requires the Central Bank to act as a Bank recording in its ledgers the issued CBDC as its liabilities while performing the settlement of the transactions and the management of relationships as the onboarding activities and the monitoring of the accounts.
The Indirect Model shifts the focal point of the distribution system to the Private Sector (e.g. Commercial Banks) which holds the role of the main actor in the full cycle of the CBDC being in charge of issuing it and managing the transaction among users. In this case, the Central Bank still guarantees the conversions between CBDC and cash while also monitoring the gross amount of deposits in the intermediaries' accounts.
The Hybrid Model requires a mutual division of roles between the Central Bank and the Private Sector. In this configuration, the Central Bank acts as the CDBC issuer while also managing the settlement of the transactions. These features imply that the CBDC is recorded as a liability of the Central Bank and also thanks to transactions management activities the Central Bank will always be aware of the total amount of the CBDC stock within the system. On the other hand, the Private Sector acts as the CBDC's distributor to the end-users and the curator of relative relationship management.

Architectural Models

A second step in the development of a CBDC environment regards the technological framework that the system will rely on. Two options are usually identified: rely on the entire system on a traditional central-based ledger or developing an Environment that purely relies on DLTs, "a database distributed in identical copies among the nodes that compose the environments. The peculiarity of DLTs is that the ledgers among the nodes chain are simultaneously updated through a consensus mechanism. The node's network is in charge of the maintenance of the ledgers implying the continuous update of the information stored in the registries."[22]Considering the possible Distribution Models explained a Permissioned Private DLT, a Digital Ledger where the transaction validator role is in the hand of the Central Authority (typically the Network owner), could be the best feasible for the Direct and the Hybrid models where the transaction management is directly in charge of the Central Bank, while for the Indirect Model it could also rely on Permissioned Consortium DLT where the validators are chosen between a set of trusted validators. Consid-

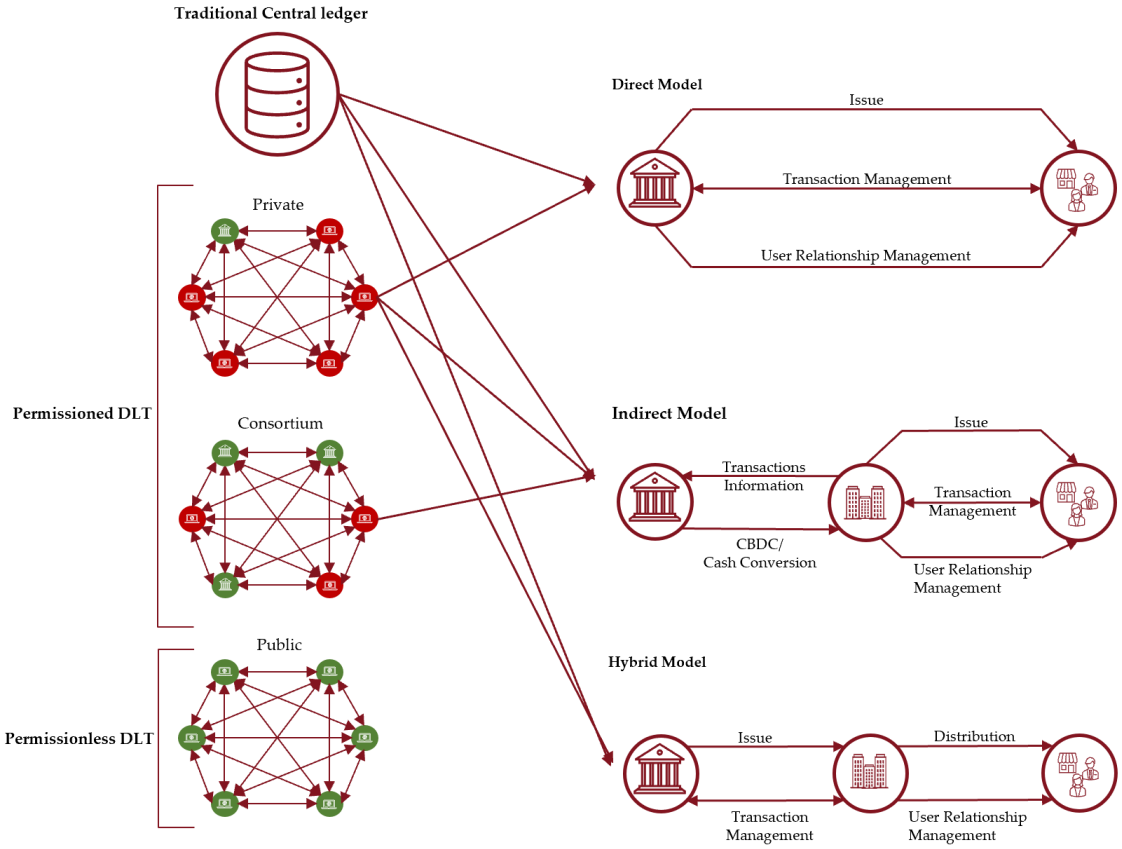


FIGURE 3: Architectural Models

ering the role of the CBDC, the application of a pure Public Permissionless DLT, where every actor of the network works as a validator through the application of a consensus mechanism, seems to have more than one technical issue. In particular, it could highlight the scalability of transactions and the reduction in speed generated while managing simultaneous high transaction volumes. The configuration that could be reached by implementing a system that relies on a Permissioned Private DLT is much more similar to the scenario where a Central Traditional Ledger is applied.

Accessibility

A third important feature in designing a CBDC Environment regards the way in which there are accessible to the users. The options swing between:

- **Account-Based Model;**
- **Token-Based Model.**

The Account-Base Model is essentially the typical commercial Bank's model that links the claims deposited into an account to a specific user's identity. In this case, the model relies on the principle "I am so I own"[3]. The Token-Based Model, similar to what happens in the Blockchain, relies on cryptography authentication methods and requires the knowledge of a private key in order to access to CBDC account. It is clear that this last configuration permits a higher degree of privacy level for the users as the information stored in the ledgers regards only the transaction flows while the user's identity is registered as an alphanumeric code. On the other hand, the traditional Account-Based Model permits, nevertheless a lower degree of privacy level, an easy-to-perform KYC and AML controls.

Potential Benefits

The rise of CBDCs could mean a significant shift in how we approach economics, offering a range of potential benefits across different aspects of the financial system. In particular, there are specific aspects where CBDCs could bring substantial advantages:

- **Financial Inclusion;**
- **Financial Innovation;**
- **Cross-Border Transactions;**
- **Transaction Transparency.**

The development of a CBDC could significantly boost financial inclusion in those systems where the population faces several issues with being part of the traditional bank system. In developing countries, a significant portion of the population could not benefit from typical services related to traditional bank activity, such as payment services and deposit accounts, due to various reasons, including the costs of maintaining a bank account and difficulties in providing necessary documentation. A CBDC environment through the development of specific Digital Wallets could ease the possibility of accessing a vault that stores digital money and a way to perform digital payments without the need for a bank account. In this way, the financial system could reach that part of the population that is historically "unbanked" (In 2021, nearly 1.4 billion adults lacked access to a bank account) guaranteeing the possibility to access basic financial services. Following the concept of financial inclusion and considering that, in 2023, nearly 6.9 billion people worldwide have smartphones, a Central Bank (considering a direct or a hybrid distribution model) could develop its own mobile application, offering basic services such as

money deposits and payment services, thus helping the unbanked population bypass the traditional banking system. The People's Bank of China (PBoC) has already developed its own application for the Digital Renminbi, and the European Central Bank has already defined that in case of the development of the Digital Euro will be developed a "ECB App" that will offer the core services defined under the Digital Euro Scheme[23]. The development of a Central Bank links also with the boosting of financial innovation that CBDCs could bring to the financial system. The introduction of a digital infrastructure that supports the CBDC could operate as the catalyst effect that will foster financial innovation within payment solutions and money management. Considering in particular the indirect and the hybrid models relying on the Private Sector for managing several activities related to the CBDC environment (e.g. Distribution, KYC, AML) could encourage the development of several innovative solutions to meet the market needs with beneficial effects also on the competition of the market. The financial innovation related to the introduction of CBDC could also foster the improvement of the current Cross-border transactions market. Except for the inside European Union transactions, domestic payment systems across the world are not interoperable with each other and often require the actions of several intermediaries in order to assess and close the transactions, thus the introduction of CBDC could cut off most of these actors linking the users directly and also having a rebound effect on reducing the transaction costs. Additionally, having an entirely digitalized environment could support the financial authorities and the private sector in mitigating the risks related to tax evasion and money laundering.

Implications for the Bank System and Political Economy

Since the beginning of the theorizing on the issue of CBDC, the literature has pointed out several potential implications for both the Bank Sector and for the Political Economy. The main issue regarding the banking system is related to the potential increase in liquidity risks, disintermediation, and possible bank runs that could be addressed by the introduction of a CBDC. In particular, the introduction of a digital central bank money, guaranteed by a Central Bank, that could be stored in digital wallets which, even in those models where the private sector could open and manage digital wallets of the users, are segregated from the bank's capital could encourage a shift into users preferences moving their deposits to a less risky alternative, the digital wallets. It is clear that a reduction of bank deposits in favor of CBDC's Digital Wallets could severely affect the bank funding activity with rebound effects on the related lending activity. In fact, a reduction in deposit amounts could force banks to fund their activities through more expensive funding sources. The use of expensive market instruments, such as debt issues, to raise funds could tighten the credit offer with negative effects on the whole economic system. On the other hand, relying on Central Bank Loans "they would have to give the Central Bank enough collateral, which would drive up the price of secure assets and change their market rates."[25]Other than that, the possibility of moving money digitally from deposits to digital wallets without any specific limitation could boost the risk of faster and more contagious bank runs. In the definition of the main Features of a CBDC, two main variables could be manipulated to mitigate the risks that the banking system could face:

- **CBDC Limit Detention;**
- **CBDC Remuneration.**

The limit detention could regard both the limitation with an upper limit to CBDC detention and the maximum amount that could be withdrawn. The detention limits could also distinguish between households and firms, for example, the actual possible design for the Digital Euro states that there will be differences in the detention limits between private citizens (still not disclosed the upper limit) and business users that "will be set a zero holding limit, which implies their impossibility of detaining Digital Euro amounts stored in their account"[23]. The effect that a detention limit could have on the European banking system has been studied by M.Azzone and E.Barucci[1] which under the assumption of a capped adoption scenario (substitution of 647 billion euros of deposits with a personal detention limit of 3.000 Digital Euros) showed that the introduction of a CBDC should negatively affect the bank's deposits with a reduction of less than 10% of the total deposits amount. Also, a scenario with a no remunerated CDBC will bring a lower loss for the mass of the deposits with a non-significant probability for bunk runs. The remuneration of the CBDC plays, as well as the detention limit, a key role in the possible decisions of the users in terms of preference between CBDC or bank deposits. As stated before a non-remunerated CBDC could lower the negative effects on the banking systems. Despite that PBoC has designed the e-CNY in this way, the ECB has declared that the Digital Euro will not bear any interest, and several other projects have moved in this way (e.g. Sand Dollar, E-Naira) an interest-bearing CBDC is still possible. However, to avoid the users'shift from bank deposits to CBDC, several constraints on the possible remuneration that the CBDC should grant need to be considered. U.Bindesil[4] has proposed a two-tier model that will help to encourage the detention of a certain amount of CBDC for payment purposes, but not as a direct substitute for bank deposits, and on the other hand will discourage its detention for investment purposes. The idea is that under a certain amount of money, the CBDC will grant the maximum rate between 0 and the Deposit Facility Rate -1%, which will ensure a minimum remuneration for the CBDC detained for payment purposes that will still be less than the bank deposits one. Exceeded the defined amount of the interest grant for the CBDC will shift to the minimum between 0 and the Deposit Facility Rate -1%, which will ensure a "punitive" treatment for those who detain too much CBDC.

- If CBDC Detained < detention threshold : $i_{CBDC} = max(0, R_{DF} - 1\%)$;
- If CBDC Detained > detention threshold : $i_{CBDC} = min(0, R_{DF} - 1\%)$.

With this configuration, a regime with high rates will always guarantee remuneration for the CBDC detentions that don't exceed the threshold that won't surpass the one paid by the bank's deposits. Under a regime of low rates, the competitiveness of bank deposits will be guaranteed by the absence of remuneration for the CBDC amounts under the detention threshold. Moving to the implications that issuing a CBDC could have on the Political Economy plan of a Central Bank, we should distinguish between the effects of the retail CBDC and the wholesale CBDC. The introduction of a CBDC into the economic system could lead to a shift into the detention preferences of households and businesses that could prefer to fund digital wallets with CBDCs instead of detaining cash in their pockets or bank deposits. The implications of the possible shift in preferences could lead to severe causes affecting money velocity, bank disintermediation (as stated before), and the number of reserves detained in the Central Bank. The digital nature of CBDC could easily affect the monetary exchanges in the economic system as digital payments do not have the same physical barriers that characterize cash exchanges and also the set-

tlement and the accounting of monetary units on the digital wallet will occur with a lower lag than the necessary time to deposit cash into bank accounts. Considering the Velocity of Money as:

$$V_t = T_n / M.$$

Is easy to figure that the increase of exchanges T_n driven by the digital nature of the CBDC could lead to an increase of the Velocity of Money, this could break the relationship between money and inflation affecting the monetary targeting of the Central Bank. In fact, looking at the relation between the Monetary Mass and the PIL of a country defined by the equation:

$$M_t x V_t = P_t x Q_t;$$
$$P_t = (M_t x V_t) / Q_t,$$

where:

- M_t: Money Mass[5];
- V_t: Velocity of Money;
- P_t: Average Price Level;
- Q_t: Production.

We can state that the average price level increases with increasing in the total money volume ($M_t x V_t$). So considering the Money Mass as a variable under the control of the Central Bank, is it clear that the possible quick growth of the transactions that a digital, unconstrained, central bank currency could carry should bring a steepen in the inflation levels. Other than that, the introduction of a retail CBDC could modify the cost configuration related to cash management, lowering the costs of banknote printing, carry and distribution but opening up to new costs arising from the CBDC implicit structure. "Depending on these changes in seigniorage income, central banks might increase or decrease their reliance on government funding, impacting their independence in shaping monetary policy"[23]. As already stated, the introduction of a CBDC could drive to a decrease in bank deposits, among everything this could also bring to a reduction of the reserves that the commercial banks held in the Central Bank with effects on the Open Market Operations. On the other hand, the introduction of a wholesale CBDC won't affect the monetary policy effectiveness but will bring a shift in the market structure redesigning the composition of the Central Bank liabilities through a decrease of commercial bank's reserves and a contextual increase of the wholesale CBDC. The considerations reported make clear that Central Banks should take several precautions before issuing a CBDC, in particular fixing threshold and limitation on both detention amounts and the transactions could hurt the demand for the CBDC but on the other hand could ensure the stability of the whole financial system. In the same way, careful policies regarding the remuneration, such as a two-tier rate configuration or a non-interest-bearing CBDC, of the CBDCs could help avoid an increase of both disintermediation and liquidity risk.

History and Development of the Digital Renminbi Project

Concerning the practical development and testing of its capabilities, significant progress on the e-CNY project was confirmed in November 2019 by Fan Yifei, the former deputy governor of the People's Bank of China (PBOC). He stated that major tasks such as high-level design, standard formulation, and functional research and testing of the legal digital currency had been completed. Pilot tests took place in various cities across China in the following years. The selection of pilot locations for the e-CNY R&D project considered factors such as major national development and regional coordinated development strategies, in addition to city-specific industrial and economic characteristics considerations. The goal was to verify the reliability of theories, the stability of systems, the usability of functions, the convenience of processes, the applicability of scenarios, and the controllability of risks.
In April 2020, the cities belonging to the "China's Silicon Valley": Shenzhen, Suzhou, Xiong'an, and Chengdu were announced as the first batch of pilot cities to enter the program. In the following months, the PBOC entered negotiations with internet companies, including ride-hailing major Didi Chuxing, to test the use of the digital currency. This effort positioned the nation as a pioneer in experimenting with the e-CNY. Didi Chuxing stated that it had inked a strategic partnership deal with the Digital Currency Research Institute of the People's Bank of China to explore the use of digital Renminbi in the smart transportation sector. Additionally, the PBOC contacted the major food delivery company Meituan Dianping, in Beijing, to discuss the pilot program and the related promotion plans across the entire platform. Other companies, such as video broadcasting websites Bilibili, also announced his active participation and cooperation efforts. To further stimulate the usage of e-CNY, in October, the PBOC distributed digital "red envelopes" containing a total of 10 million e-CNY to 50.000 citizens in Shenzhen. The e-CNY could be spent in Shenzhen's Luohu District at merchants that had completed the digital RMB compatibility transformation. Citizens gained access to these red envelopes through a lottery system. The 3,389 participating merchants, including restaurants, supermarkets, gas stations, metro stations, department stores, and other businesses that had completed the digital RMB compatibility transformation, allowed recipients to spend the gifted amount between the 12th and 18th of the month. This incentive method will also be implemented on future multiple occasions and in various cities as a means to encourage the usage and familiarity with the Digital RMB.
The pilot test advanced in its extension further in November with the inclusion of Shanghai, Hainan, Changsha, Xi'an, Qingdao, and Dalian as pilot areas, representing the second batch of digital RMB pilot testing cities. For some of the mentioned cities, the e-CNY project was integrated and developed as part of the cities' respective five-year development plans. These plans are comprehensive frameworks crafted by local governments to delineate economic, social, and environmental goals, along with initiatives to be accomplished over a five-year period, in alignment with national priorities. For instance, Shanghai enthusiastically embraced participation in the program, aligning with its involvement in the "14th Five-Year Plan for Comprehensively Promoting Urban Digital Transformation in Shanghai" Fintech innovation project. The primary objectives of this initiative included the promotion of new financial technologies, enhancement of financial industry efficiency through digitalization, improvement of institutional service levels, and enhancement of convenience and inclusiveness in financial services. Similarly, the "14th Five-Year Plan for the Development of Hainan Province's Financial Industry" advocated for the launch of e-RMB pilot projects across the island, aiming to explore application scenarios of e-RMB tailored to the characteristics of the "Hainan Free Trade Port" initiative. The comprehensive objective of the latter is to transform Hainan into a global hub for free trade, thereby facilitating international exchanges more effectively. The Digital RMB could significantly contribute to achieving this objective by enhancing the efficiency and transparency of

[5]The total average nominal amount of money in circulation in the economy.

cross-border payments, reducing associated costs, ensuring traceability and supervision of cross-border capital transactions, and promoting the development of new offshore international trade and related business activities.

A key milestone regarding the promotion of the e-CNY among private companies, and more specifically, e-platforms, occurred when the second-biggest online retailer giant Jingdong (JD.com) became the first of its category to accept payment in digital Yuan. On December 11, 2020, JD.com distributed 100.000 digital cash vouchers, totaling 20 million yuan, to residents of Suzhou for use on specific items available in their store.

In February 2021, to implement the action plan for the Winter Olympics of science and technology and strengthen the payment service environment for the Beijing Winter Olympics, the People's Government of Dongcheng District, in Beijing, hosted the "Digital Wangfujing Ice and Snow Shopping Festival" digital RMB pilot activity. This festival was designed to integrate digital RMB usage across various consumption scenarios related to the Winter Olympics. As part of this initiative, 50,000 digital RMB red envelopes were distributed to winners through appointment registration and lottery distribution, with each red envelope containing 200 Yuan. Winners were able to spend this digital RMB at designated merchants in the shopping street of Wangfujing and within the festival activity area at Jingdong Mall. This pilot activity showcased the practical applications of digital RMB in a festive and consumer-oriented setting, highlighting its potential role in enhancing payment services during major events.

Another significant advancement in the progress of pilot testing occurred in March 2021 with the promotion of the digital RMB currency wallets on the app of the six major state-owned banks: The Industrial and Commercial Bank of China, Agricultural Bank of China, Bank of China, Bank of Communications, China Construction Bank, and Postal Savings Bank of China. Customers interested in participating in the promoted pilot test could apply either by visiting a branch of the participating banks or by enrolling in a whitelist, scanning the provided QR code, registering on the e-CNY app, and opening the sub-wallet. Initially, there would be a daily cumulative payment limit of 1.000 Yuan, with the option to apply for an upgrade in the future.

"As of June 30, 2021, e-CNY was applied in over 1.32 million scenarios, covering utility payment, catering service, transportation, shopping, and government services. More than 20.87 million personal wallets and over 3.51 million corporate wallets had been opened, with transaction volume totaling 70.75 million and transaction value approximating RMB34.5 billion"[31]. Meanwhile, as of October of the same year, "approximately 140 million Chinese residents had opened a digital Yuan account through either payment or banking apps, with accumulated transactions reaching 62 billion Yuan since its launch. Mu Changchun, the head of the Digital Currency Research Institute, said in November"[13].

Starting from January 2022, the digital RMB pilot version app became publicly available on app stores such as Apple, Huawei, Xiaomi, Vivo, and Oppo for residents of the cities where the pilot program was being conducted. Following its release, the app quickly ranked among the most downloaded apps in the subsequent days, reflecting significant interest and adoption among users in these areas.

During the Beijing Winter Olympics, the digital Renminbi garnered international attention and interest. In all the areas and related provinces of Beijing and Zhangjiakou where the games took place, consumers could use the digital Yuan not only at the Olympic venues but also for a variety of services, including transportation, catering, accommodation, shopping, sightseeing, healthcare, telecommunications, and entertainment. People from around the world could all use it via smartphone apps, or with wearable devices such as wristbands , or even ski gloves . Additionally, special ATMs were strategically installed for this purpose. These ATMs were equipped todirectly convert up to 18 types of foreign currencies (e.g.: Euro, US Dollar, Swiss Franc, Norwegian Krone) into Digital RMB. Users could insert banknotes into the machine, confirm the amount and exchange rate, and then receive a physical card from the ATM, which served as a physical digital RMB wallet. In terms of privacy protection, the PBOC governor, Yi Gang stated that data collection concerning the CBDC would adhere to the principle of "anonymous for small-value and traceable for large-value transactions."[16], assuring that the volume of data collected for the CBDC would be lower than that of existing e-payment instruments. In terms of figures, as estimated by a senior official from the PBOC, the e-CNY facilitated payments of 2 million Yuan or more per day during the Winter Olympics.

After the Olympics, the PBOC widened the scope of the digital Yuan pilot program by incorporating 11 additional cities. These new pilot areas encompassed Tianjin, Chongqing, Guangzhou in Guangdong Province, Fuzhou, and Xiamen in Fujian Province and, additionally, six cities dedicated to host the Winter Games - Hangzhou, Ningbo, Wenzhou, Huzhou, Shaoxing, and Jinhua - were included, marking them as the third batch of pilot cities.

In December, the fourth and final batch of pilot cities was introduced, encompassing the city of Jinan, Nanning, Fangchenggang, Kunming, and the Xishuangbanna Autonomous Prefecture. During the same month, Alipay integrated the digital Yuan into its services ecosystem, including platforms like Taobao for online shopping, Ele.me for food delivery, Freshippo for grocery retail, and the Shanghai Public Transport system. On the e-CNY app, users were enabled to set both single payment limits and daily cumulative payment limits for transactions conducted via Alipay utilizing the digital Yuan.

In May 2023, a remarkable development occurred in Changshu: public sector workers in the city began receiving their entire wages exclusively in digital Yuan. The policy affected government employees and staff at state-owned companies and public institutions, such as schools, hospitals, libraries, research institutes, and media organizations within the city. According to the Chinese state media, this rollout represents the largest implementation of the digital Yuan recorded thus far. Later, in July, the Bank of China, China Telecom, and China Unicom jointly collaborated to launch the SIM card hard wallet product within the digital yuan app. Available only to Android mobile phone users, the SIM card hard wallet integrates a super SIM card with the e-CNY soft wallet. Users only need to install a super SIM card issued by the operator on their mobile phones, log in to the e-CNY APP, open a SIM card hard wallet, and use the Near Field Communicatio (NFC) function of the mobile phone to complete the e-CNY payments.

The Digital Renminbi has made significant progress compared to the digital euro. The PBOC has expanded its pilot programs rapidly, covering various cities and scenarios, including public sector payrolls and large-scale events like the Beijing Winter Olympics. Technologically, the e-CNY has introduced features such as the SIM card hard wallet, enabling offline transactions and demonstrating a robust infrastructure supported by major tech and financial institutions. Collaboration with the private sector, such as integrating the digital Yuan with Alipay and Taobao, highlights China's seamless blend of public and private efforts to promote the currency. In addition, China's proactive user adoption initiatives, including distributing digital cash vouchers and usage campaigns, further demonstrate

its advanced position in CBDC deployment. The Eurosystem's back-end prototype, named NXT, utilized an unspent transaction output (UTXO) data model, a common framework for digital currency transactions. This system demonstrated its capability to support various types of transactions while safeguarding users' privacy by not disclosing their payment patterns or account balances to the Eurosystem. Concurrently, market participants successfully implemented and tested all five payment scenarios, exploring innovative approaches such as self-custody wallets, which could potentially enhance privacy pending future legislative developments. The exercise also served to technically assess the interface between the front-end and back-end layers, with results indicating smooth interaction. However, it is important to note that since all prototypes were developed entirely from scratch, the exercise did not account for the potential effort required to adapt existing payment service provider (PSP) systems. Looking ahead, the future steps for the Digital Euro involve finalizing the legal framework, ensuring financial stability measures, determining the appropriate technology for the settlement system, and addressing security and integration concerns. On June 28, 2023, the European Commission presented a regulatory proposal to ensure the legal tender status of the digital euro. The acceptance of this proposal is crucial for its widespread acceptance and distribution across the Union, aiming to bring the appreciated features of cash into the digital sphere and ensuring that the digital euro adds value for people. The investigation phase clarified several issues, including measures to ensure the financial stability of the Eurosystem and to avoid bank disintermediation effects. There will be a limit on digital euro holdings for private users, which will be disclosed just before its issuance, and a zero holdings limit for business users to prevent its use as an investment instrument. Additionally, a remuneration system for digital euro holdings will not be implemented to discourage its use as an investment tool. The ECB has not yet disclosed the underlying technology for the back-end settlement system of the digital euro. The options being considered include the implementation of Distributed Ledger Technology (DLT), reliance on traditional technologies, or a combination of both. The ECB will prioritize the security level of the technology and the feasibility of integrating it with existing end-user services.
In summary, it can objectively be stated that the e-CNY is ahead in practical deployment, technological integration, and user adoption compared to the digital euro, which remains in the early stages of development and has yet to be introduced to the EU citizens.

Financial Inclusion

As discussed in the previous chapter, the development of a Central Bank Digital Currency (CBDC) could be pivotal in promoting financial inclusion in countries where traditional banking methods are not readily accessible. The barriers vary, encompassing geographical challenges, income disparities, gender gaps, and educational levels, among others. Such difficulties become more pronounced in a rapidly growing nation like China, which needs to maintain the pace of development while simultaneously improving the quality of life. According to the World Bank[32], financial inclusion refers to "The uptake and usage of a range of appropriate financial products and services by individuals and micro and small enterprises (MSEs), provided in a manner that is accessible and safe to the consumer and sustainable for the provider". Nevertheless, to analyze the level of financial inclusion globally, four key elements are inherent in all these definitions, namely:

- **Accessibility:** Consumers access financial products easily via physical branches and digital devices;
- **Diverse and appropriate products:** Financial products and services are tailored to meet consumer needs and can be readily selected and utilized as required;
- **Commercial viability and sustainability:** Financial providers offer profitable and sustainable products, services, or models, striving for balanced economic, environmental, and social impacts through efficient management;
- **Responsibility and safety:** The policy of financial inclusion should align with those of financial stability and market integrity.

Globally significant progress has been made in expanding the scope and ambition of financial inclusion, with China achieving remarkable results. According to the Global Findex Database 2021[10] and as illustrated in the graphs below, over the past decade, euro area bank account ownership has risen from 90% to almost 99% of adults and from 40% to 71% in developing economies (fig. 4). China mirrored this upward trend, from 64% to nearly 89% of individuals owning a bank account. Furthermore, a similar upward trend is observed in the usage of digital payments. In the Euro Area, the percentage of adults who made or received a digital payment increased from 88% in 2014 to 97% in 2021 (fig. 5). This trend is also evident in developing countries, including China, where COVID-19 served as a catalyst for this growth. Indeed, 82 percent of chinese adults made a digital merchant payment in 2021, with 11% doing it for the first time since the beginning of the pandemic. However, the progress in financial inclusion is not yet complete. Based on these statistics, most individuals who can easily open a bank account have already done so. Thus, the next steps are:

- Enhancing inclusive financial policies to connect rural customers with the internet, government, and the private sector;
- Improving the range and quality of financial services available to those who already have a bank account.

Three key players have shaped and will continue to shape financial inclusion in China. Firstly, the fintech companies, led by two of the world's largest holding groups: Tencent and Alibaba. Through their e-commerce and fintech companies, they have introduced numerous financial innovations. Secondly, traditional financial service providers, which often maintain a focus on offering standard products to their customers. Finally, the Chinese government with PBOC and other financial sector authorities, whose policies govern the behaviors of the other stakeholders. Policies can support the actions of other stakeholders or take a different direction, as demonstrated by the development of a Central Bank Digital Currency (CBDC). In the following sections, there will be a more in-depth exploration of the topics discussed:

- Section 2.1 outlines the Chinese landscape that facilitated the rapid diffusion of digital payments and e-CNY;
- Sections 2.2 and 2.3 explore the government's solution to financial inclusion, digital renminbi;
- Section 2.4 includes a brief conclusion.

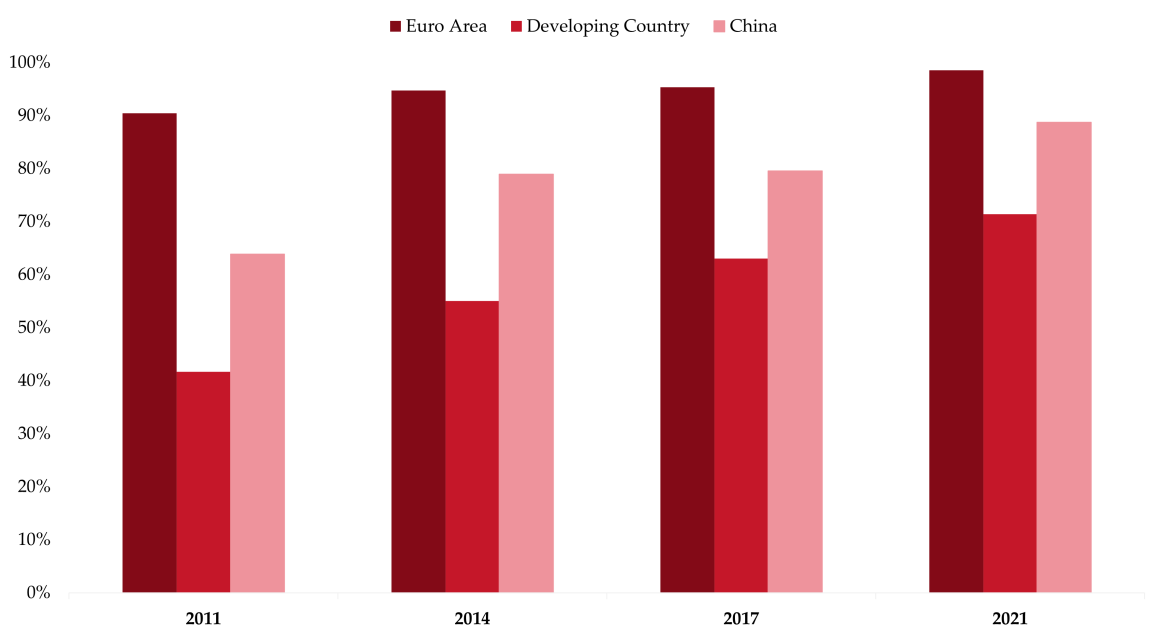


FIGURE 4: Accounts (% age 15+)

Chinese Landscape

Why is China so advanced in the development and use of new digital payment methods? Why does financial inclusion appear to be more progressed in China compared to other countries? As previously mentioned, the case study of the e-CNY is unique within the panorama of CBDCs due to its advanced stage of development and its reach to millions of citizens. Thus, what are the reasons for this upward trend? First, it is necessary to give a detailed description of the Chinese social structure, what are the main stakeholders and how are they characterized. The main stakeholders that shaped the financial inclusion in China are:

- **Chinese citizens.** They are the first utilizers of technological innovations, such as digital finance or e-CNY. Their characteristics and their needs are the reasons for the evolution of new digital payment methods or for better policies.
- **Chinese regulators and authorities.** Since the establishment of rural credit cooperatives in the early 1950s, the Chinese government and the People's Bank of China (PBOC) have consistently focused on expanding access to financial services for their citizens. However, this heightened attention has recently led to the implementation of restrictive policies, particularly targeting specific subareas such as online lending and consumer loans[30]. Nevertheless, the most significant advancements in financial inclusion have been realized through the development and utilization of the People's Bank of China's CBDC, e-CNY.
- **Financial services providers.** Traditional providers such as banks, along with new types of providers like microcredit companies and fintech firms, serve as the driving force behind financial inclusion by offering competitive and innovative financial solutions. In this context, Alipay and WeChat emerge as the predominant players, boasting a collective user base of nearly 2 billion individuals in 2018[19]. Alipay holds approximately 50% of the market share in China, while WeChat Pay 40% [14].

Chinese Citizens

With almost 1.5 billion citizens, China is the second most populous country in the world[39]. This, coupled with a low population density of 152 people per km^2, results in a significant divergence between urban and rural areas. In fact, in 2023, 35% of all Chinese citizens lived in rural areas rather than in cities. Moreover, despite boasting a high level of nominal GDP, the average wealth of Chinese citizens is not commensurately high, with a GDP per capita of $11,449 in 2022[40]. Nonetheless, the country demonstrates consistent improvement annually and could be categorized as an emerging economy. This demographic and economic landscape provides essential context for understanding the state of financial inclusion in China. The table above (tab. 1) presents statistics from the 2021 Global Findex database[10] on individuals owning a bank account, categorized by geographical region and various demographic characteristics. First, as stated in the previous section, China has already achieved a high level of overall accessibility to bank accounts which is way better than developing countries. However, compared to the Euro Area, there is still room for improvement. Significant disparities still exist particularly in income distribution, education levels, and employment status. Thus, it suggests that enhancing access to financial accounts for low-income individuals and those with only primary education or less will contribute to the overall progress of financial inclusion in China. Beyond account ownership, several other critical indicators of financial inclusion are depicted in the histograms above (fig. 6), which are derived from the Global Financial Inclusion Database. The first graph focuses on digital payment transactions. According to the Global Findex Database, making digital payments includes respondents who reported using mobile money, a debit or credit card, or a mobile phone to make a payment from an account, as well as those who used the Internet to pay bills or make online purchases within the past 12 months. Notably, a high share of Chinese citizens (86.2%) use digital payments, possibly due to the popularity of e-commerce, though this percentage is still below that of the Euro Area. The second graph illustrates individuals' saving habits, particularly savings at financial institutions.

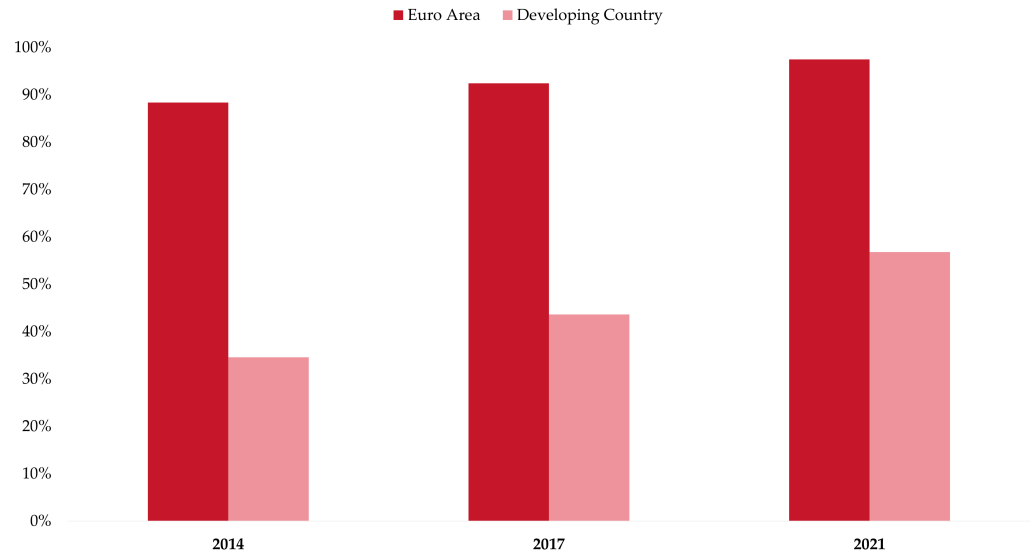


FIGURE 5: Made or received a digital payment (% age 15+)

Features	Indicators	China	Developing country	Euro area
Gender gaps	Male	89.92 %	74.20 %	98.70 %
	Female	87.34 %	68.47 %	98.31 %
Income distribution	Poorest 40%	83.08 %	66.55 %	97.38 %
	Richest 60%	92.46 %	74.59 %	99.25 %
Education level	Primary or less	83.02 %	64.76 %	96.54 %
	Secondary or more	97.21 %	78.99 %	98.93%
Age group	Ages 15-24	88.47 %	61.87 %	94.85 %
	Age 25+	88.91 %	74.22 %	98.98 %
Employment status	Out of labor force	69.10 % (2017)	56.49 %	97.84 %
	In labor force	83.41 % (2017)	70.30 %	99.03 %
Total		**88.71 %**	**76.20 %**	**98.51 %**

TABLE 1: Accounts per demographic classes (% age 15+)

The data reveals that nearly 1 in 2 Chinese citizens (44.7%) saved at a financial institution at least once in the past 12 months, which is double the rate compared to developing countries. Finally, the last histogram presents borrowing behaviors of individuals over the past 12 months. Chinese adults are more likely than those in developing countries to report having borrowed in the past year but are significantly less likely to have done so compared to adults in the Euro Area.

Chinese Regulators and Authorities

China's financial inclusion landscape has evolved through different policies ruled by various Chinese regulators, such as the government and the PBOC. The creation of rural credit cooperatives (RCCs) in the early 1950s set the start for an explicit financial inclusion policy. However, by the early 2000s, the effects of marketization and financial sector reforms had resulted in the closure of tens of thousands of financial service providers in rural areas. This left rural credit cooperatives (RCCs) and the postal savings system as the primary sources of financial services for rural residents. Moreover, at the 2006 National People's Congress, these problems were encapsulated and emphasized by the Three Rural Issues (agricultural, rural, and farmers' issues), or sannong, which highlighted the economic challenges faced by peasants in rural areas since 1990. Therefore, Chinese financial sector authorities began to focus on three main areas:

- Universal access to basic banking services;
- Productive credit for rural households;
- Bank credit for micro and small enterprises.

To achieve these objectives, the China Banking Regulatory Commission approved the creation of the Postal Savings Bank of China (PSBC) in 2007, a full-fledged state-owned commercial bank [9]. Its goals were to promote financial inclusion by deploying agent-based service points and adapting services to meet the diverse needs of rural consumers. Nowadays, the PSBC offers a variety of finan-

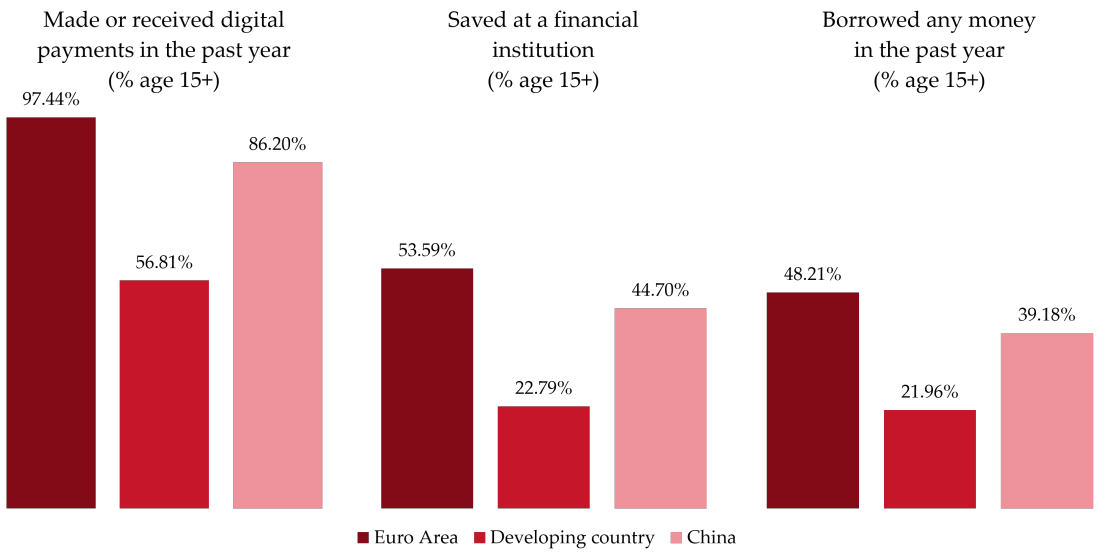


FIGURE 6: Other metrics

cial services, including minimum livelihood guarantee payments, grain subsidies, rural medical insurance subsidies, utility payments, remittances, e-commerce services, loan applications, and investment counseling. This makes PSBC the most broadly represented financial service provider in rural China[27]. Simultaneously, another state-owned commercial bank was founded in 2009[35], the Agricultural Bank of China (ABC). The bank has been at the forefront of implementing the government's three-pronged policy aimed at supporting the agricultural sector, rural communities, and farmers (sannong). In recent years, ABC has made significant advancements in product and service innovation to better serve these areas. For example, ABC developed various nonland-related collateral, such as farming equipment, agricultural inventory, and direct grain subsidies, to facilitate secured lending in rural areas. It is important to mention the China Banking Regulatory Commission (CBRC), established in 2003[26] to regulate China's banking sector. In 2018, it merged with the China Insurance Regulatory Commission (CIRC) to form the China Banking and Insurance Regulatory Commission (CBIRC)[26]. Additionally, the CBRC, in collaboration with the People's Bank of China (PBOC), has organized and supported numerous outreach, training, and knowledge development activities related to movable. finance product development, often in partnership with the World Bank Group's International Finance Corporation (IFC). In addition to these regulatory authorities, the Chinese government together with the central bank, PBOC, also have actively taken a wide range of policy measures to promote financial inclusion, through monetary and credit policies, tax policies, and supervision policies. More in detail, PBOC has encouraged financial service providers to extend credit services to rural communities (sannong) and micro and small enterprises (MSEs) through a range of policies, including differentiated reserve ratios, loan refinancing, and rediscounted loans. Finally, in 2015, the State Council issued China's Plan for Advancing the Development of Financial Inclusion (2016-2020) (FIP), which reaffirmed certain policy objectives aimed at advancing financial inclusion.

Financial Services Providers

The last significant social stakeholders in the Chinese financial inclusion landscape are the financial service providers, as summarized in the table below(tab. 2). Depending on their nature, each provider can be categorized into one of these three types:

- **Traditional financial services providers** (e.g. commercial banks, rural credit cooperatives);
- **New type providers** (e.g. village and township banks, microcredit companies);
- **Fintech companies** (non-bank digital payment providers, P2P lenders and internet-based financial services).

Traditional financial service providers. Have been pivotal in advancing financial inclusion in China. Under policy guidance from the Chinese government, these providers have greatly extended the physical reach of their service networks, modernized the country's payment infrastructure, and introduced product-level innovations, often through partnerships with fintech companies. Consequently, there has been a substantial increase in the adoption and usage of financial products, particularly bank accounts and bank cards. One example is the Rural Credit Cooperatives (RCCs). Starting from 1950s, RCCs have undergone various reforms over the years, the most significant occurring in 2003 when RCCs were no longer required to maintain their cooperative ownership structure, governance, or business operations. This reform led to the creation of two new institutional forms: Rural Commercial Banks (RCOMBs) and Rural Cooperative Banks (RCOPBs). By the end of 2016, 1,125 RCCs were operating in China, along with 1,154 RCOMBs and RCOPBs that had transitioned from RCCs following the 2003 reforms[32]. However, several challenges continue to limit RCCs' role in financial inclusion, including poor governance, small customer bases, excessive local authority interference, and limited capacity for innovation. Consequently, RCCs are losing appeal in favor of new fintech companies.

New type providers. Between 2006 and 2008, the Chinese government introduced regulations to establish "new type" rural financial service providers, including village and township banks (VTBs), rural mutual credit cooperatives (RMCCs), and microcredit companies (MCCs). The policy objective was to increase financial inclusion among traditionally underserved and unserved customers. Establishing these new rural providers can be seen as an ex-

Category of Financial Service Provider	# of Providers	Total Assets (Billion Usd)	Total # of Branches	Regulator
State-owned commercial banks	5	12990	68953	CBRC
Joint-stock commercial banks	12	6521	15366	CBRC
City commercial banks	134	4236	16156	CBRC
Rural Commercial Banks (RCOMBs)	1114	3040	49307	CBRC
Rural Cooperative Banks (RCOPBs)	40	65	1381	CBRC
Rural Credit Cooperatives (RCCs)	1125	1193	28285	CBRC
Insurance companies	203	2268	-	CBRC
Village and Townships Banks (VTBs)	1443	186	-	CBRC
Microcredit companies (MCCs)	8673	-	-	Local government
Nonbank digital payment providers	266	-	-	PBOC
P2P lending platforms	3709	-	-	CBRC

TABLE 2: Financial Service Providers

tension and complement to ongoing efforts to strengthen the role of RCCs in serving the agricultural sector, rural communities, and farmers (sannong), as well as a mechanism to promote competition in rural financial services. These new-type rural financial service providers are characterized by differentiated and lighter requirements for registered capital, organizational structure, and ownership arrangements. According to the World Bank Group[32], these providers have had numerous positive effects. They have improved access to rural finance, filled gaps in financial services in rural areas, and reduced farmers' and micro and MSEs' reliance on civil society finance, thereby enhancing the financial environment in rural regions. Despite these positive outcomes, challenges remain, such as limited innovation, high management costs for VTBs, and MCCs' limited differentiation in market positioning from commercial banks.

Fintech companies. The most recent actors in Chinese financial inclusion are the emerging fintech companies. In recent years, China has become a global leader in fintech innovation. New entrants to the financial sector have introduced novel models, delivery channels, and products, leveraging the massive scale and network effects of online e-commerce and social media platforms. The rapid growth of fintech companies in China can be attributed to their ability to meet the unmet demand from consumers and micro and small enterprises (MSEs) that were often overlooked by traditional financial service providers focused on state-owned enterprises. Additionally, the proliferation of fintech in China has been fueled by advancements in technology, such as the Internet, smartphones, digital payments, Artificial Intelligence, and Machine Learning, along with initial promotion and legitimization by the Chinese government and institutions, with a "wait and see" approach. However, Chinese regulatory authorities have recently become more restrictive, issuing targeted regulations to ensure safe and supervised innovation, along with a more centralized financial power. This results in more restrictive entry barriers for new companies and consolidates the position of early movers. Two of the most significant early movers are Ant Financial Group and Tencent Holdings Limited. These large financial groups own various entities operating in the fintech sector. For instance, they own the top two nonbank digital payment providers with the highest payment volume in 2019: Alipay and WeChat Pay[30]. Additionally, they offer other internet-based microlending services, such as Ant MCC, which provides small loans to agricultural households in rural areas, and internet banks like WeBank and MYBank. With this wide range of different financial services, Ant Group and Tencent hold dominant positions in China's digital finance sector and both companies have significantly expanded financial inclusion. However, recent regulatory actions, such as the mandated separation of Jiebei and Huabei services into distinct corporate entities[15], may significantly undermine their influence in digital finance. These regulations are issued to prevent financial instability that could arise from such a duopoly, which might lead to increased transaction costs or higher credit and investment fees, anyway, thanks to the collaboration and efforts of these stakeholders, China has emerged as a global leader in digital payments.

Digital Renminbi for Financial Inclusion

Another approach the Chinese government adopted to foster financial inclusion in the country is the development of the digital Renminbi, e-CNY. It also intends to support fair competition, which is mainly dominated by the duopoly described before. Furthermore, with the decline in cash usage for retail payments due to the rise of the digital economy and cryptocurrencies, a new state-based digital currency with a legal tender could offer greater safety, universality, and inclusivity for citizens. The digital RMB system is designed to further lower the barrier to public access to financial services compared to alternatives like Alipay and WeChat Pay. For instance, it operates without requiring a bank account and does not necessitate KYC (Know Your Customers) procedures for small amounts of e-CNY. Moreover, because its operations are governed by the state, cannot be negatively affected by new regulations. Finally, another crucial advantage is the absence of interest charges for using e-CNY as a means of payment. Anyway, MyBank and WeBank announced their plan to incorporate e-CNY as a payment option on their platform, enhancing interoperability between these major providers[15]. More details about the digital renminbi app and its functionalities will be provided in the next chapters. Thus, the full rollout of e-CNY offers several key benefits:

- **Increased interoperability.** Both Alipay and

WeChat Pay could integrate e-CNY into their wallets, enhancing the compatibility between various intermediaries;

- **Enhanced financial security.** In the event of major disruptions among intermediaries, the PBOC can ensure the payment system remains operational;
- **Broader accessibility.** e-CNY enables digital payments in areas with physical and social barriers;
- **Issuing subsidies.** e-CNY can be utilized to distribute state subsidies directly to the accounts of citizens requiring financial support.

On the other hand, there are significant concerns regarding the potential negative implications of e-CNY on financial inclusion in China. First, despite numerous regulations aimed at limiting other financial service providers, the duopoly of Alipay and WeChat Pay still maintains substantial market share and influence. These platforms can now extend their reach to unbanked individuals, potentially offering additional financial services that may not be necessary. Second, it remains uncertain how much rural areas and citizens will benefit from e-CNY. Although, according to ABDInstitute[15], some rural citizens still lack of bank accounts and/or a stable internet connection. Third, the legal and regulatory framework for financial consumer protection requires further adaptation to ensure comprehensive coverage of consumer protection risks associated with fintech and digital finance. Specifically, there is a critical need for a robust legal framework for data protection and privacy.

Chinese Financial Inclusion: Conclusions

The Chinese financial inclusion landscape has flourished, thanks to the concerted efforts of all stakeholders. First, the role of the government and regulators has been pivotal. Implementing a robust and comprehensive financial ecosystem is essential for enabling financial inclusion. The government initially adopted a "wait and see" regulatory approach to foster the development of new digital finance models, which were subsequently actively monitored to mitigate consumer risks. Second, financial service providers have significantly contributed to financial inclusion. Traditional providers, following government policies, have expanded their networks and modernized payment infrastructure, though challenges such as limited innovation capacity remain. New-type providers have improved access to finance in rural areas but faced high management costs. Emerging fintech companies, led by Ant Financial and Tencent, have utilized technology to meet the demand from underserved consumers and small enterprises. However, recent regulations aimed at maintaining financial stability may limit their influence. In conclusion, despite these challenges, China's coordinated efforts have positioned it as a global leader in digital payments and financial inclusion.

The Architecture of the Digital Renminbi

Two-Tier Model Analysis

Deepening the CBDC architecture topic is crucial to fully understand the different relationships between Central Banks, Commercial/Retail Banks, and end-users (e.g., consumers, small/medium businesses, and large corporates) while identifying the flow of information and legal claims amongst the multiple entities. Focusing on how the architecture of the digital Renminbi is designed, it is possible to note how it is to all intents and purposes an indirect architecture, consisting precisely of 2 main tiers. Going into more detail:

- On the first tier, the PBOC will issue and redeem e-CNY to commercial banks and other permitted organizations, including telecommunications corporations and already-existing mobile payment systems (Alipay and WeChat Pay). Among the responsibilities of the PBOC are wallet ecosystem management and digital currency issuance and disposal. This makes the e-CNY legal tender. As a result, the People's Bank of China Law has been amended to implement this management structure, extending the legal tender of the physical Renminbi to its digital form and emphasizing the PBOC's exclusive right to issue the Renminbi.
- Instead, the second layer consists of commercial banks and other approved institutions in charge of providing e-CNY to the general population. To be more specific, the authorized operators work together to jointly provide e-CNY circulation services and retail management under the PBOC's quota management. This includes innovative payment product design, system development, scenario expansion, marketing, business processing, operation, and maintenance.

Accordingly, to this system infrastructure, users must reach commercial banks in order to get e-CNY via a digital wallet; by doing this, PBOC is able to avoid becoming an intermediary in the Chinese financial system. It also lessens its obligations and risk exposure in this manner as well. Moreover, to fully harness the energy and inventiveness of all parties engaged and preserve the stability of the financial system, the PBoC will work to guarantee that there are fair playing conditions and that the market has a crucial role in how resources are allocated. In fact, this two-tier operating model may effectively leverage the resources, skills, and technological advantages of designated operators to achieve market-driven, innovation-promoting, and competitive selection of the best.
In addition, for what concerns the operating system, the digital Renminbi includes four different mechanisms[2]:

1. **Issuance**
   The issuance mechanism is the first one to be implemented. It starts with the commercial banks that must apply to the central bank in order to have their applications for digital RMB approved. The commercial banks apply to the central bank, which carries out uniform monitoring and approval of such applications. Consequently, the accounting system department will deduct the commercial banks' deposit reserves.
2. **Repatriation**
   Through the digital RMB repatriation mechanism, the central bank receives the digital RMB deposited by the commercial banks. It then deposits the amount and performs several storage or cancellation operations. Following the commercial banks' submission of an application for a digital RMB deposit, the central bank completes the ensuing approval order and partially completes the cancellation process. Then the accounting system department starts the deposit reserve increase command and deducts the corresponding amount from the reserve ratio. After the completion of these activities, it notifies the commercial bank that the return has been completed.

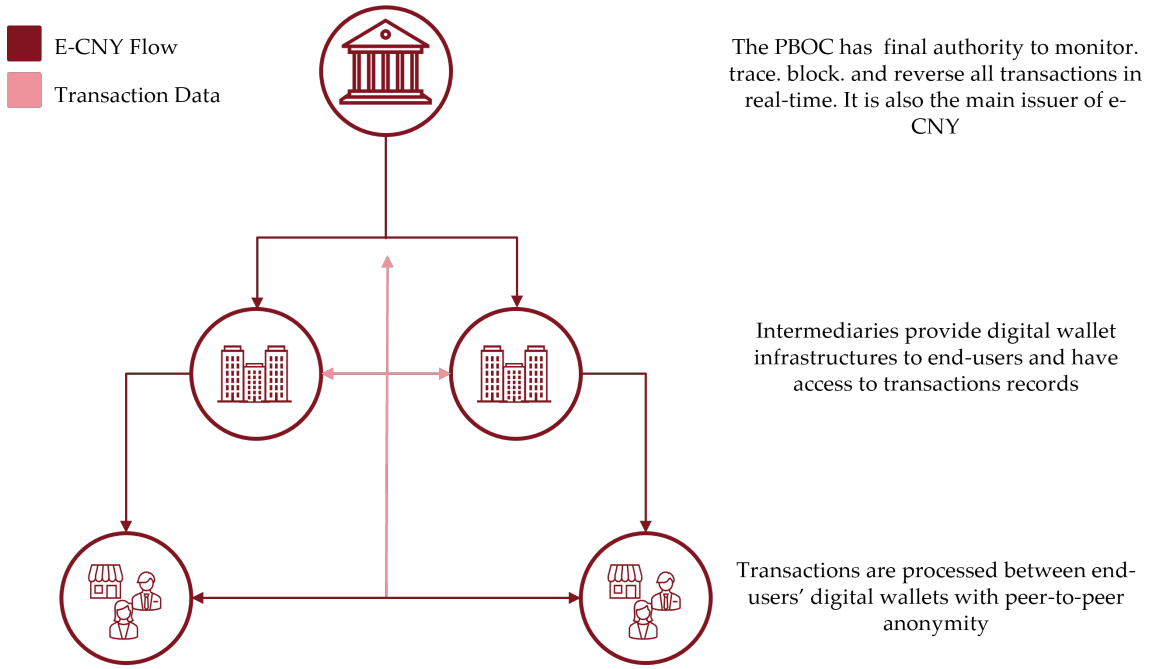


FIGURE 7: Explanation of the two-tier architecture of the Digital Yuan, [15]

3. **Transfer**
   Moving on, the digital RMB transfer mechanism describes how digital RMB can be moved from one commercial bank, A, to another, B. The central bank will complete the subsequent nullification plan after bank A submits the transfer request. Based on the amount of money to be transferred, commercial bank B will generate RMB legal tender coins. If after the coins are nullified, there is still a balance of such coins, the central bank will realize the remaining amount and send the RMB legal tender coins to commercial banks A and B, respectively.
4. **Settlement**
   The last kind is the digital RMB payment mechanism, wherein the user primarily transfers digital RMB using a digital RMB wallet and wherein the transaction records from the data nodes are stored at the central bank data center. Furthermore, if the payer and the receiver are both offline the e-wallet records the transaction procedure to proceed with the transaction at a later time.

The latter mechanism gives an idea of the crucial role played by the digital wallet, the importance of which will be analyzed and explored in more detail in the following chapter.

Technical Specifications

In this section, a deeper analysis of the e-CNY technical specifications will be conducted. Specifically, it is possible to state that, although some of the PBOC partners may decide to use distributed ledger technology (DLT), the e-CNY adopts a technology-neutral distribution. Indeed, the e-CNY can be transferred via digital data strings and has a variable face value, acting as a currency alternative. Tencent's (WeChat Pay) and Alibaba's (AliPay) proprietorial technologies form the foundation of its digital payment infrastructure. These make use of digital wallet-connecting QR codes. The customer shows a QR code on their phone upon payment, which the retailer scans to validate the transaction. Subsequently, funds are moved from the user's virtual account to the merchant's account. The retail CBDC can benefit from the QR code technique. This is because a buyer needs to obtain a form of payment and have it approved at the time of sale for a transaction to be completed effectively. After that, there needs to be a money exchange (in digital form) with the vendor. It must also be possible for the seller to utilize it as payment in subsequent transactions. The hybrid technical foundation of the e-CNY is based on the existing Chinese retail QR infrastructure. It makes use of distributed infrastructure and the digital wallets and QR codes discussed before. The framework is defined as follows[6] :

- **Hybrid technical framework:** The technological foundation for the e-CNY is hybrid. Its distributed infrastructure from its Tier 2 banks is combined with a Tier 1 centralized architecture. It is possible to co-develop functionality with this support for both an agile and steady state.
- **Distributed Infrastructure:** Decentralized payments are made possible by the distributed infrastructure of Tier 2 banks, which uses DLT protocols to provide simultaneous access, validation, and record-keeping. The Tier 2 banks use their computer network and several nodes or sites, usually connected via the Internet, to accomplish this.

The Digital Wallet

A pivotal role in the architecture of a CBDC is played by the digital wallet as it composes the primary interface between the digital currency and the end user. The Public Bank of China (PBOC) is responsible for stating the rules related to the whole set-up of a wallet eco-platform, based on centralized management, unified cognition, and anti-counterfeiting. Specifically, they authenticate e-CNY and realize wallet ecological platforms to qualify special features in order to satisfy the different types of demands of different users at different levels. On the other hand, according to the two-tier organizational system built up for

	Cat.1	Cat.2	Cat.3	Cat.4	Cat.5
Sign up	In person	Remote	Remote	Remote	Remote
Authentication	ID and phone number	ID and phone number	ID and phone number	E-mail and phone number	E-mail and foreign phone number
Connected account	Yes	Yes	No	No	No
Balance limit	None	500.000	20.000	10.000	1.000
Transaction limit	None	50.000	5.000	2.000	500
Daily limit	None	100.000	10.000	5.000	1.000
Annual limit	None	500.000	100.000	50.000	10.000

TABLE 3: *Digital Wallets: Types&Features*

the e-CNY, authorized operators jointly develop and share apps on mobile devices.
These intermediaries detain the digital wallets, and they categorize them according to the strength of the customer's identification and his necessities. e-CNY wallets are stored in the home-banking apps of such operators and users can reload their portfolio directly from them. These movements of cash clearly depend on the information obtained by the intermediaries related to the owner of the wallet regarding his financial reliability. By default, users open anonymous wallets with the lowest privileges, which can be upgraded to real-name wallets with higher privileges as needed[11].
With the aim of a rapid and successful spreading of the digital currency, these wallets need to be user-friendly and furthermore to be accessible to everyone, also to the less acknowledged people. For this purpose, the wallet's interface resembles many popular contemporary digital payment apps in China, such as Alipay or WeChat Pay. Typical features already used for the above-mentioned applications such as QR code scanning or biometric authentication may become the usual practice also for the e-CNY wallet authentication and the approval of the transactions between them. It will be also possible to transfer digital yuan from one wallet to another by simply touching two phones together. On the strength of the fact that e-CNY is generated directly by the PBOC (and so it is considered legal tender), every type of transaction that involves the digital yuan must be accepted and this currency carries settlement finality, which means that payments made using the digital yuan are settled upon payment. In addition to that, payments in digital yuan may be preset in time in a similar way that happens with credit cards (i.e. through application programming interfaces).

Main Characteristics

Regarding the functionality of the transactions, a digital wallet exploits security chips and other technologies to enable the functions of e-CNY. These wallets are based on Integrated Circuit (IC) cards[6] and they may be supported by mobile phones, wearable objects or other Internet of Things devices.
Other important characteristics that could increase the appeal of such a wallet are the ability to merge with the already existing financial platforms[7] by including the connection to investment portfolios or permitting automatic bill payments; insertion of regulatory functions suggested by regulators directly into the wallet, i.e. automatic tax deductions, constant monitoring in order to avoid possible frauds or compliance with international sanctions. Moreover, these wallets may add multiple secondary functionalities to their basic backbone such as insurance products or microlending. As a consequence, this would lead to a larger offer and range of opportunities by commercial banks.

Loosely Coupled Account Links

Probably, the most relevant feature is the feasibility of transactions happening between two e-CNY wallets without the need for them to be associated with a bank account or to be connected to the Internet. The PBOC refers to this particular system as loosely coupled account links which was designed primarily to make e-CNY function more like cash and so, as said before, to ease the dissemination and use of the digital currency even for that slice of the population that is less technologically savvy.
As stated in PBOC's 'Progress of Research & Development of e-CNY in China' released in July of 2021, e-CNY claims "to meet the public demand for anonymous small value payment services based on the risk features and information processing logic of current electronic payment system[s]" This ensures that difficulties arising from technological illiteracy or geographical limitations are minimized to meet people's needs in order to create a structured but highly usable operational system that can secure business continuity. Therefore, this innovation in terms of transactions is aimed at building up a new and efficient financial framework without binding people to disengage too much from the usual payment systems they use in everyday life.
Thanks to this, offline and online transactions are both feasible. While the latter ones are obviously supervised by the PBOC who acts as a transaction validator, the possibility of offline settlements may lead to think that, for these specific cases, they can happen without any limits or regulation. However, this is not properly true: transactions are anonymous vis-à-vis third-party intermediaries, such as commercial banks and internet platforms, but the PBOC and other authorized entities can see them. This is called

[6] An IC (Integrated Circuit) card is a payment card, typically made of plastic, that incorporates an embedded microchip to store data, replacing or complementing the traditional magnetic stripe.
[7] Both Tencent and Alibaba have announced the integration of Digital Renminbi on their platform, which are respectively WeChat pay and Alipay.

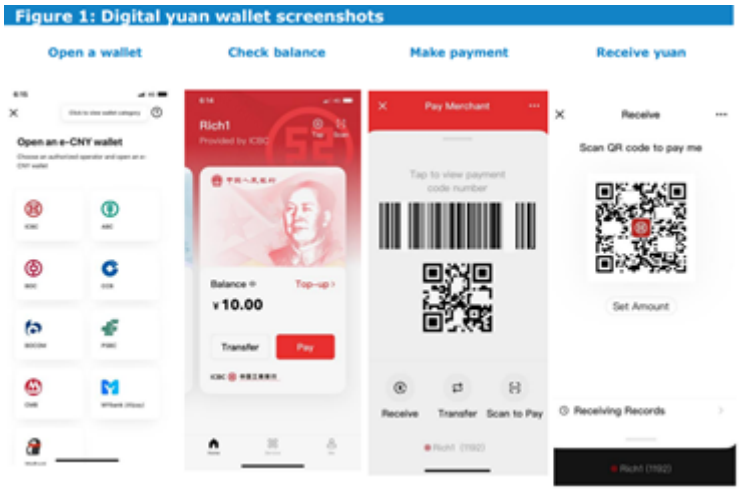


FIGURE 8: Four screenshots of digital yuan wallet interface[7]

manageable anonymity since, from one side, the PBOC has still the right to increase or decrease the level of a transaction and even, if necessary, deactivate a wallet if illegal or just suspicious manoeuvres are detected, but, at the same time, some steps involving the online banking system are overcome. Despite that, the technical features related to the transmission of data are not fully disclosed yet to the Central Authority, so it is not known, as of today, how the entire process in offline transactions works.
A key mention has to be made to the different levels of anonymity depending on the weight of the transaction. To quote Mu Changchun[29] , the director of PBOC's Digital Currency Research Institute, "The anonymity of the central bank's digital currency is limited under the premise of controllable risks. However, it is possible to make small payments using anonymous wallets linked to cell phone numbers. To conduct digital yuan transactions of large amounts, consumers will have to undergo KYC (Know-Your-Customer) verification procedures." Small value payments can be conducted in a simple way without KYC standards while large ones require users to perform KYC.

Different Types of e-CNY Wallets

According to the information received by the authorized operators, different types of wallets are generated, and they can vary from user to user in, for example, the limits of daily transactions as well as a maximum balance. In this way, PBOC and the other entities involved can maintain an efficient control architecture and people who usually do not need to move large amounts of money can still keep a high level of privacy.
In the same way, users can customize their wallets to have functions that meet their needs and their financial possibilities. The effort put in by the PBOC to create tailor-made wallets for the customers is yet another attempt to build an easy-to-use scheme for all people.
In particular, digital wallets seem to have three key dimensions:

- **Software and Hardware**
  A main subdivision in the digital wallet architecture can be done according to how customers may access to them. In particular, software wallets provide services through mobile payment apps, software development kits (SDK), application programming interfaces (API), and so on. On the other hand, a hardware wallet is based on security chips and other technologies in order to realize e-CNY-related functions. Such chips are supported by IC cards, cell phone terminals, wearable objects such as badges, bracelets, gloves, or smart watches, and the Internet of Things devices. This combination of hardware and software ensures that the whole wallet ecosystem is well-designed to grant the availability of the digital currency and to meet the wishes of different people.
- **Personal and Corporate**
  Digital wallets may differ also on the type of subject of their opening. Ordinary people and self-employed individuals can access to personal wallets whose strength is determined by the information collected regarding the subject (I.e. they may vary on transaction, balance, and daily limits). In a similar way, corporate wallets can be opened by legal persons or unincorporated organizations: in this case, the limits are calculated according to whether they are opened in person or remotely. There may be further possible customizations in order to suit the needs of the users: the hierarchy of these portfolios depends on how much information users want to provide (in case they want to make large amounts payments or keep higher balances).
- **Parent and Sub**
  An additional split refers to the possibility to set up a main wallet (which will be called parent) and open a few sub-wallets under it. These can be subject to payment caps, payment conditions, personal privacy protection, and other functions that can be set by customers. Furthermore, sub-wallets may be exploited by enterprises and organizations to distribute their funds and manage their finance in the most efficient way. The opening of sub-wallets is encouraged by e-CNY: through the use of tokenization and encryption, online merchants such as e-commerce platforms or O2O (online-to-offline) can isolate their personal information from other tech companies and so protect users' privacy.

Digital Wallets in China: Statistics

The main focus of the People's Bank of China, together with the designated operators and all the relevant organizations, is creating a well-designed wallet architecture to meet the needs of multiple scenarios and perceive their

	June 2021	October 2021	December 2021	May 2022	August 2022	June 2023
Personal wallets	20.87 Mln	140 Mln	261 Mln	n/a	n/a	120 Mln
Corporate wallets	3.51 Mln	10 Mln	n/a	n/a	n/a	n/a
Transaction numbers	70.75 Mln	150 Mln	n/a	264 Mln	360 Mln	950 Mln
Transaction value	RMB 34.5 Mln	RMB 62 Bln	RMB 87.6 Bln	RMB 83 Bln	RMB 100.04 Bln	RMB 1800 Bln
Avg Transaction value	RMB 488	RMB 413	n/a	RMB 314	RMB 278	RMB 1895

TABLE 4: *e-CNY Pilot Statistics[20]*

own distinctive functions. The loose coupling between the e-CNY wallet and the bank account reduces the dependence on financial intermediaries in the transaction process and allows for anonymity for small-value payments.
In July 2023, Yi Gang, China's central bank governor, released an update on some statistics regarding the usage of e-CNY digital wallets among customers[20]. According to Mr. Yi, more than 20.87 million personal wallets have been opened by individuals and organizations and over 3.51 million corporate wallets, with transaction volume totalling 70.75 million and transaction value approximating RMB 34.5 billion given the first data collected in June 2021. Due to the shortage of information available, it was not possible to find any details related to the percentage of parent and sub wallets opened in the last years.
Further information was given related to the number of CBDC wallets, which should be around 120 million. Previous reports, actually, talked about 300 million wallets, so it is possible that Mr. Yi was speaking of active e-CNY wallets instead of opened ones.
Although the number of digital wallets seems to have decreased in time, the amount of transactions has hugely increased to 950 million along with the average transaction values which suggests that the usage in corporate cases had a considerable boost in the last few years (predictable since the Shanghai Clearing House announced it would support the digital yuan for wholesale commodities transactions).
Not only from the point of view of the architecture of digital wallets but in general for the whole CBDC structure, China seems to be the most developed and most advanced country, especially in contrast to Europe which still has great strides to make to reach the level of the Asian superpower.

Differences between the Digital Euro Scheme and the Chinese Model

According to what was initiated and seen in the previous paragraphs, the models taken as reference in our consideration find not only similarities but also obvious differences. These, in this regard, are particularly due to cultural and jurisdictional characteristics; about the structures on which these models rest, however, it is possible to find elements of similarity. We leave the examination of these aspects to the next lines of this section.
In order to deeply analyze the different keys of comparison, it's possible to set the aim of the discussion starting from and considering the following structure: *Background*, *Design*, *Functionalities*.

Background

Standing initially on considerations about the regulatory and perimeter background, clear differences between the two digital currencies in question appear. It is possible, in fact, basically to consider the earlier birth and the consequent greater development of the latter over the former, that is, of the Digital Renminbi over the Digital Euro; in this sense, standing on the main consideration of the normative perimeter publication, a White Paper on research and development has been issued during 2021, establishing the scopes and elucidating the PBOC's stance, the context, goals, and aspirations, outline the design framework, and address policy considerations concerning the e-CNY system. On the European side, since the origin of the concept in 2020, ECB has aimed to reduce this well-known gap with China as much as possible by establishing the preparation of ad hoc regulatory frameworks and initiating related study and development phases: after years of research, the ECB entered the Preparation Phase of the Digital Euro project in the last November (2023), phase in which has been stated and confirmed that the Digital Euro is expected to actually launch in 2027; in spite of this, dealing again with the e-CNY, its experimentation has already been conducted on individuals.

Design

In the present section, various elements of difference between the two currencies can be analyzed, albeit with some similarities in some aspects; it's possible to start with the general structures and the scopes. In this sense, just like the Digital Euro, the e-CNY is designed to reflect the functionality of physical RMB, serving as a direct claim on the central bank and backed by sovereign credit. Primarily catering to domestic retail payment needs, it operates, as already said, on a two-tier architecture, albeit with a not-so-clear infrastructure and access systems as per current public information. Notably, its design is attuned to mitigate the risks of financial disintermediation, hence devoid of interest and subject to quantitative limits through a tiered wallet mechanism.
The two-tiered (or indirect) structure represents an element of differentiation from the one implemented by ECB, which relies upon a "hybrid model" accepted by the European Commission in 2023; this assumes that the digital currency is directly issued by ECB, while the private sector provides its distribution and end-user relationship. Given this consideration, the Chinese model can still be considered as a kind of hybrid but is slightly diverging from the direct provision of consumer accounts by the central bank; in fact, the PBOC distributes the e-CNY to authorized and selected operators, such as commercial banks and other financial intermediaries, who will subsequently provide it to consumers along with exchange and circulation services. Despite seemingly amplifying the authority of China's Central Bank over commercial banks, this architecture does not entirely exclude commercial banks or private payment tools (like WeChat or Alipay).
With these infrastructure considerations being made, it is worth mentioning that its functional system substantially

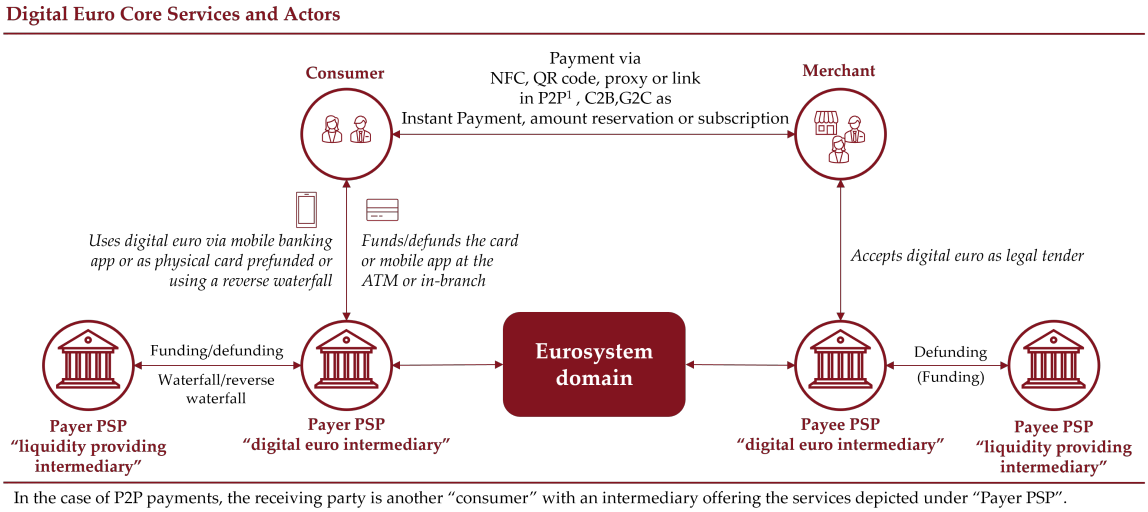


***FIGURE 9:** Main services and actors of Digital Euro[12]*

deals with blockchain technology, standing on a centralized methodology; even for this case, Eurosystem is currently exploring centralized and decentralized approaches, such as distributed ledger technologies but, however, a decision on this side has not yet been made. In particular, it could be mentioned that ECB conducted a prototype exercise from July 2022 to February 2023 in which has been tested the Digital Euro back-end prototype for online payments, known as NXT: differently from a distributed ledger, NXT's structure is based on a UTXO (Unspent Transaction Output) data model, a largely used instrument in digital currency transactions[23]. Continuing in the other sense, the e-CNY functions on a centralized-permissioned Distributed Ledger Technology (DLT) managed by the PBOC, which records and processes all transactions: this implies that the government has complete access to transaction data and retains the authority to annul or reverse transactions as deemed necessary.
On the other hand, this represents and opens a clear discussion point on the privacy issue; in particular, a few lines will be spent on this topic below. The position of the EU to protect users' privacy has been widely declared and, in this sense, we could find in it another element of diversity. Providers of e-CNY services use to classify customer information into "general" and "sensitive" categories. However, commercial banking policies often lack clear guidelines on handling sensitive e-CNY user data. While China's Personal Information Protection Law (PIPL) applies to digital currency service providers, the absence of specific operational procedures in commercial banks' pilot policies may create regulatory gaps in protecting sensitive e-CNY user information. Therefore, the use of e-CNY transactions does not offer complete anonymity, as the PBOC retains access to transaction data for security purposes; this lack of anonymity is due to currency registration and traceability being inherent in e-CNY transactions. The People's Bank of China can exercise comprehensive oversight over the currency's usage through data mining and big-data analysis. However, the effectiveness of this oversight in controlling tax evasion, money laundering, and terrorism financing is questionable, as most illicit activities do not occur through formal monetary channels, as stated by Bank for International Settlements. On the other hand, although still in the formative stage, the European Data Protection Board (EDPB) clarifies that privacy rules will be extensively specified. It also notes that solutions will be adopted that, however, cannot guarantee complete transaction anonymity; therefore, to meet the privacy protection objective, "privacy thresholds" will be set, i.e., limits below which neither offline nor online low-value transactions are traced for anti-money laundering and counter-terrorism financing purposes.
The EDPB and the EDPS (European Data Protection Supervisor) emphasize that the proposed Regulation should further clarify the data protection responsibilities of the ECB and PSPs: this includes the legal bases on which the ECB and PSPs should rely and the types of personal data they should process for the issuance, distribution, and use of the Digital Euro.

Another point of discussion stands now on the theme of interests' generation. According to this, the PBOC White Paper demonstrates a keen awareness of the potential hazards of financial disintermediation: for instance, the e-CNY neither accrues interest nor related payment, mitigating competition with commercial banks. Moreover, the e-CNY operates within a comprehensive framework encompassing big data analysis, risk monitoring, and early warning systems; while not overtly stated, this framework may imply a precautionary measure preventing withdrawals from commercial bank deposits into e-CNY during periods of financial instability. As far as Europe is concerned, it seems to be addressed on the same path: within the framework of its Regulation, the Digital Euro won't generate interest payments. In a parallel field, it's possible to present another similarity between the two currencies, reaching the topic of "internationalization". In this sense, ECB has announced that, following a success behind the launch of the Digital Euro in the Euro Area, it will commence studying and endorsing the technical feasibility of implementing cross-currency and cross-border functionalities, aiming for multiple objectives. Ultimately, even though it would be primarily intended for domestic use, the e-CNY is considered technically ready for cross-border transactions. In this field, the PBOC White Paper adopts a prudent stance regarding the potential utilization of the e-CNY in cross-border payments or for advancing RMB internationalization. Indeed, China has initiated a collaborative initiative with the Bank for International Settlements (BIS), along with Hong Kong, Thailand, and the United Arab Emirates, to explore cross-border CBDC transactions facilitating almost instant settlements beyond conventional payment infrastructures.
In closing the present section, it's added that the Digital

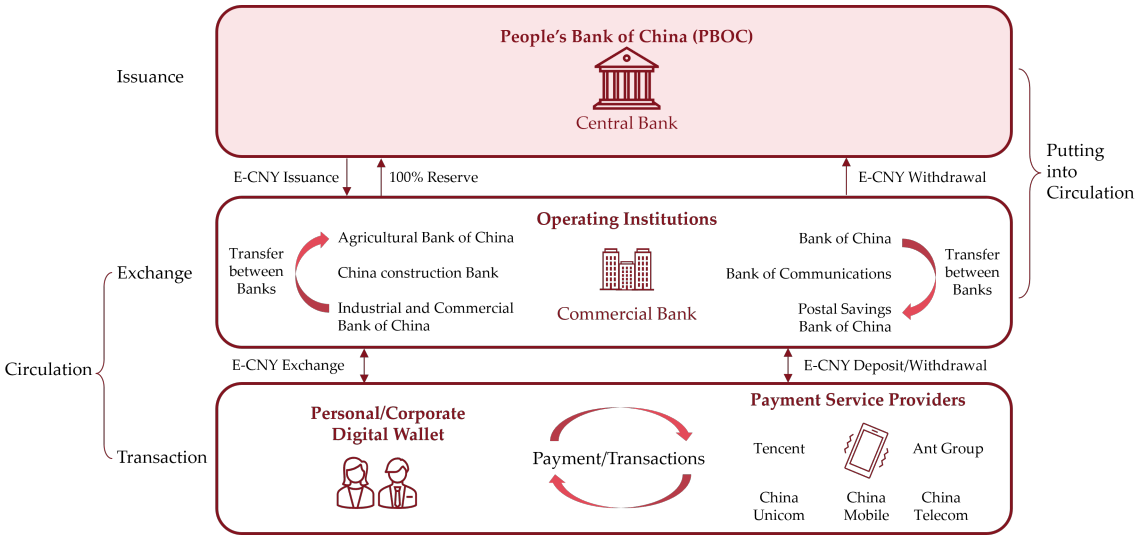


***FIGURE 10**: The e-CNY's Two-Tier Operating System [11]*

Euro would be endowed with the status of legal tender thus requiring its mandatory acceptance in payments by all payees: in light of this, the Digital Euro should also be directly accountable as a liability for the ECB. This similarity further aligns it with the Digital Renminbi.

Functionalities

In initiating this section, the specific functionalities, though in some ways shared, between the two types of currencies will be discussed, analyzing their applications, their modes of use, as well as the actors involved. As a first point, it's possible to present that the e-CNY aims to address several key functionalities as outlined in its White Paper.
One crucial feature is that the e-CNY leverages "smart contracts" to enable programmable functionalities, ensuring payments adhere to predefined conditions or terms: the just said feature could potentially restrict transactions with certain entities, such as criminal or politically undesirable ones, and facilitate targeted macroeconomic policies. Additionally, another important feature is the implementation of a tiered system of wallets, as said before, managed by authorized financial intermediaries under PBOC guidance; these tiers have varying transaction and balance limits, preventing users from emptying their bank deposits into e-CNY wallets entirely. They may present also different characteristics, such as the typologies personal/corporate, software/hardware, or a parent/sub-wallet. In general, the digital wallet, accessible via the e-CNY app, is where users manage and store their e-CNY funds; some of its advanced features may require verification with a Chinese identity card.
In a very similar way, the Digital Euro wallets should work, in particular with the maximum limit allowable and the associated identity verification, requesting a Digital Euro Account Number (DEAN). In a more general key, the typology of users can be categorized as: individual consumers, businesses and merchants, financial institutions, governments/public entities. Here, following the investigation phase, the ECB has decided to limit the holding of Digital Euros, albeit not defining precise quantitative amounts[23]. As slightly mentioned in the previous parts, on the first side, private citizens would face restrictions on the amount they can hold in their accounts, an amount expected in its dimension but still unknown. For commercial users, merchants, and public administrations, a holding limit of zero will be established with the completion of the actual preparation phase, preventing them from retaining Digital Euros in their accounts: here, this zero-holding limit will be enforced through the waterfall system that transfers any received Digital Euro payments directly to the entity's cash account; simultaneously, a reverse waterfall approach will fund Digital Euro payments directly from the entity's bank.
Concerning this topic, the ECB through its Digital Euro Scheme (DES) and Digital Euro Rulebook defines Access, Liquidity, and Transaction Management, sets of services and procedures to address Digital Euro end users, using waterfall approaches in funding and defunding wallets.
Dealing with DES, through the figure 10, it's possible to evaluate the net of stakeholders participating in the process.
Here it's necessary to mention the compensation model for the Digital Euro, a model that aims to strike a balance between providing sufficient incentives for Payment Service Providers (PSPs) to distribute the Digital Euro and ensuring adequate protection for end users.
In a parallel way, it's provided in the figure 11 a similar structure of actors' involvement for e-CNY.

Standing on the DES, it aims to maintain the Eurosystem's central role in issuing and managing the digital currency while allowing Payment Service Providers (PSPs) some flexibility in design choices to enhance digital solutions; in support of this, the ECB's Digital Euro Scheme Rulebook outlines three levels of services that intermediaries must offer: Core, Optional, and Value-added Services: Core Services, mandatory for user readiness, include payment instrument management and transaction processes; Optional Services, at the discretion of intermediaries, may include account portability and payment scheduling; Value-added Services, left to the private sector, aim to innovate and improve solutions for end users. On this last basis, it has already been observed that Chinese model leaves operational margin only for selected intermediaries, giving here another slight difference. In the will of mentioning one more point, on the side of payment programmability it is easier to find a clearer ground: China has already been active on this aspect for some time, while Europe is still in the evaluation phase, though it does not embrace an openness to it.
Wanting to conclude this section, it is possible to point out that according to what has been seen and analyzed, while there are several differences between both currencies,

there are just as many elements that unite them; or rather, unite the Digital Euro with the Digital Renminbi. By virtue of this, clear as it may be, the e-CNY currently connotes itself as one of the most developed digital currencies in the world, to whose models even the Euro, in a sense, aspires. So, although the details of this discussion have been glossed over, the main difference would seem to be precisely the time elapsed between their respective adoptions.

The Technology Behind Digital Renminbi

Digital Currencies and Cryptocurrencies: Analogies and Differences

Digital Currencies, Cryptocurrencies and blockchain technology are tightly related yet are different things. In recent years, the landscape of finance and technology has undergone a transformative evolution, propelled by the rise of digital currencies, cryptocurrencies, and blockchain technology. These innovations have not only captured the attention of investors and entrepreneurs but have also sparked profound discussions about the future of money and decentralized systems. At the forefront of this revolution are cryptocurrencies, decentralized digital assets built on blockchain technology. Bitcoin, the first and most well-known cryptocurrency, emerged in 2009 as a decentralized alternative to traditional fiat currencies, challenging the existing financial paradigm controlled by central authorities. Cryptocurrencies are blockchain based digital currencies. Blockchain refers to a distributed ledger system that enables transparent, secure, and immutable record-keeping of transactions. Unlike traditional centralized databases, blockchain operates on a decentralized network of computers (nodes), where transactions are verified and recorded in chronological order. This decentralized architecture ensures that no single entity has control over the network, fostering trust and resilience in the face of tampering or censorship. Moreover, public blockchains derive their sustainability from the computational resources contributed by miners, individuals, or entities whose primary aim is to acquire cryptocurrencies. These miners play a crucial role in the network's operations, dedicating their computing power to validate transactions and secure the blockchain. In return for their efforts, participants in most blockchain networks, excluding those privately owned, are rewarded with incentives to ensure the ongoing maintenance and integrity of the system. The incentivization mechanism within blockchain ecosystems typically revolves around the issuance of cryptocurrency tokens, such as Bitcoin and Ether, which act as rewards for miners and other network participants. These tokens serve not only as a form of digital currency but also as a mean to incentivize continued participation and contribution to the network's operation and security. However, it's worth noting that not all blockchain networks operate on this incentive model. A second framework typology involves privately owned blockchains, exemplified by IBM's Hyperledger. Such blockchains diverge from the traditional cryptocurrency-based incentive structure: in these cases, the maintenance and operation of the blockchain are overseen and managed by a central entity or organization, rather than relying on external participants seeking cryptocurrency rewards. Instead, the private owner of the blockchain assumes responsibility for its upkeep, ensuring its functionality and security without the need for external incentivization through cryptocurrency rewards.

The third category of digital currency operates independently from blockchain technology and involves utilizing internet-based transactions instead of traditional cash payments. This category encompasses various forms, including digital tokens utilized within online platforms. Examples of such digital currencies include those offered by Alipay and WeChat, and Tencent's online gaming communities (QQ Coin). While Apple Pay, a relatively recent addition to the digital payment landscape, incorporates cutting-edge technologies like Near-field communication (NFC), its payment methodology closely mirrors that of established platforms such as Alipay, WeChat, and PayPal. Apple Pay facilitates transactions by linking to users' bank accounts, thereby avoiding the creation of new currency.

e-CNY Technology

Ever since the first rumors of the digital currency from the People's Bank of China there were analogies to blockchain-based cryptocurrencies like Bitcoin, in reality such comparisons are far from justifiable, these instruments are indeed very different technology-wise. First of all, the purposes are very different, Bitcoin was built in 2009 with the intention of creating the first peer-to-peer currency that did not need any centralized authority to supervise its functioning; China on the other hand has the goal of becoming the first major economy to integrate a central bank digital currency. Designed to serve as a digital, perfect substitute for physical money e-CNY had not been developed using the same technological framework of blockchain-based digital currencies for different reasons:

- A permissionless public distributed ledger or blockchain could not be scaled due the available technology to the need of China economy, such solution would not be appropriate to manage the expected transaction volumes. According to the People's Bank of China (PBC), the Digital Currency Electronic Payment (DC/EP) system must possess a processing capability of at least 300,000 transactions per second[28]. This requirement closely mirrors the peak processing capacity of Alibaba, which was demonstrated during Singles Day 2019[33]. On that occasion, Alibaba's Apsara Operating System successfully handled a staggering 544,000 orders per second. However, current blockchain technology falls significantly short of meeting this demanding criterion. For example, Bitcoin can theoretically process only seven transactions per second, while Libra boasts a more modest capacity of up to 1,000 transactions per second [21].
- The decentralized nature of blockchain technology presents a significant challenge to the centrality of the People's Bank of China (PBC) within the country's financial system. Furthermore, it has the potential to undermine the government's control over monetary policy through the central bank. For example, in a system utilizing Bitcoin technology, the money supply would be dictated by market participants rather than by the central bank. Similarly, in a scenario resembling a Libra-type consortium, the authority wielded by the consortium would effectively supplant that of the PBC, assuming the role of a de facto central bank.
- Furthermore, the adoption of a public blockchain would enable market participants to have unrestricted access to all data stored on the ledger, which would directly contradict China's Cybersecurity Law. This law explicitly mandates that data generated within China's borders must be exclusively

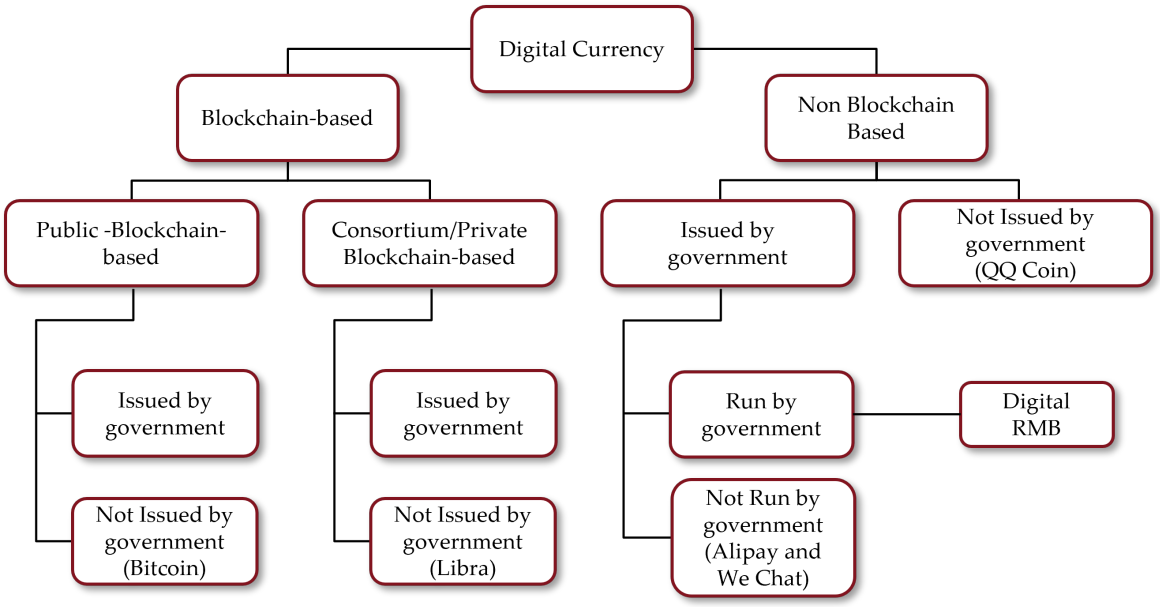


FIGURE 11: Categories of Digital Currencies

stored and processed within the country. Consequently, the People's Bank of China (PBC) cannot authorize the exposure of DC/EP transaction data to any computer linked to the public blockchain.

The PBOC, considering the constraints of public permissionless DLT, has opted, according to the e-CNY architectural model, for a technology-neutral two-tier hybrid framework where:

- **Tier 1**: Rely on permissioned Centralized Ledger which guarantees the centralized settlement of the transactions and to PBOC "the full access to transaction data and can cancel or revert transactions when it deems this to be appropriate"[15]
- **Tier 2**: "The distributed infrastructure of the Tier 2 banks facilitates decentralized payments through DLT protocols that allow for simultaneous access, validation and record keeping. In order to do this the Tier 2 banks utilize their computer network and multiple nodes or locations, typically over the Internet."[6]

To foster a technologically neutral environment, the PBOC encourages Tier 2 players to provide innovative e-CNY circulation services and user management procedures, developing innovative payment products, platforms, and business processes. Furthermore, to ensure a level playing field and foster financial inclusion, the PBOC has also developed its own e-CNY app that will provide e-CNY services to all users, including those who do not have an e-CNY digital wallet linked to a bank account.

The Use of Blockchain for CBDCs

As of today, the e-CNY stands as the sole significant instance of a Central Bank Digital Currency (CBDC) in practical operation. However, several other nations have either initiated trials or embarked on research endeavors toward the development of their own digital currencies. Some of these research initiatives have demonstrated an interest in leveraging blockchain technology. For instance, South Korea has conducted trials involving a digital won on a distributed ledger, utilizing technology from the blockchain division of the local tech behemoth, Kakao. Nevertheless, there is a prevailing consensus that blockchain technology is not imperative for the implementation of a CBDC. One notable challenge associated with public distributed ledgers pertains to scalability. Proof-of-work blockchains, such as the one underpinning bitcoin, are renowned for encountering severe bottlenecks in terms of transaction throughput, thus posing a significant obstacle to scalability.

e-CNY App

In 2014, China introduced the digital Renminbi, also known as the e-CNY, a digital version of the Chinese Yuan. Over the past decade, the project has undergone several stages of development and integration, culminating in its adoption on a global scale in 2024. In fact, China has expanded access to the digital Renminbi application to more than 210 countries and regions. Notably, on March 18, 2024, the People's Bank of China published a user guide to facilitate the use of the app by foreign visitors as well.

Currently, the app offers five main features:

- **Wallet Opening and Management:** Users can easily open and manage their e-CNY wallets through the application by registering and using a phone number from one of the 210 enabled countries and regions, without the need for a bank account, visiting a bank branch, or presenting identification documents. However, in this case, the limit for each transaction will be 2.000 CNY and 5.000 CNY per day. Beyond this, users are free to set parameters such as daily spending limits and link different bank cards.
- **Wallet Reload:** The digital wallet can be reloaded using various options, including payments with international credit cards, local bank cards and even foreign currency bills[36].
- **Peer-to-Peer Payments:** Users can transfer small sums of money from one user to another, allowing virtual currency to be used for non-business transactions as well.

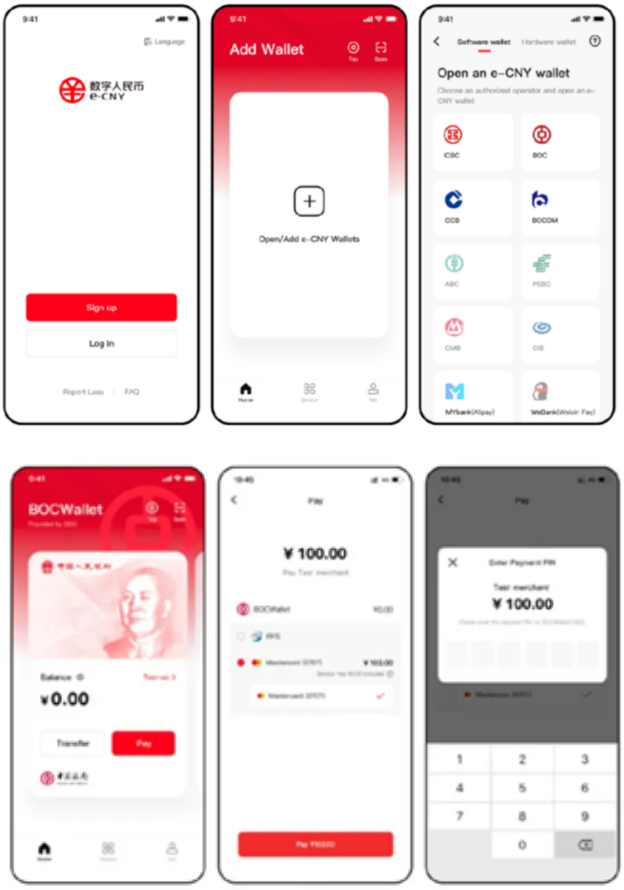


FIGURE 12: e-CNY APP [36]

- **Online and At Merchants Payments:** The e-CNY can be used to pay for goods and services online and at merchants who accept this form of payment, thus offering a wide range of spending options such as "Scan to pay" and "QR Code Payment"[37].
- **With the e-CNY app**, users can request a card or hardware wallet for wearable devices directly from their phones. Simply log in to the app and visit the dedicated section. This new feature allows users to easily connect their cards and hardware wallets to wearable devices for even simpler management. Additionally, with Mobile Pay, available for Android phones, users can make payments even when the phone is off, offering an unparalleled level of convenience. Users can check their device's compatibility by visiting the Hardware Wallet page in the e-CNY app. Furthermore, those who own a super SIM card from China Mobile, China Telecom, or China Unicom can open a SIM card wallet directly from the e-CNY app on their Android phones[38].

Foreign visitors can now register on the e-CNY app using their international phone numbers, streamlining the process of accessing and using e-CNY. A Chinese ID card is required to access advanced wallet options. The wallet, linked to a bank account and equipped with ID card verification, has a single payment limit of 50.000 yuan, a daily cumulative limit of 100.000 yuan and a maximum balance of 500.000 yuan. On the other hand, anonymous transactions can be carried out using the wallet, which has a single payment limit of 2.000 yuan, a daily cumulative limit of 5.000 yuan and a maximum balance limit of 10.000 yuan[18].
China has introduced a new feature for foreigners, allowing them to top up their e-CNY digital wallets before making payments, thereby enhancing their experience with the digital yuan payment system.

Differences between using International Cards Linked to WeChat Pay and Digital RMB (e-CNY) in China

With the growth of payment options in China, foreigners are faced with several options. Among them, linking international cards to WeChat Pay and directly using digital RMB (e-CNY) represent two practical solutions, but with distinct characteristics.

- **Link international cards to WeChat Pay:** Allows credit or debit cards issued outside China to be linked to WeChat Pay. This option is particularly useful for temporary visitors, although it may be subject to limitations imposed by banks or regions, and incur additional costs for currency conversion.
- **Digital RMB payments (e-CNY):** Allows the user to directly use digital currency issued by the People's Bank of China, eliminating exchange rate issues. This method requires the installation of a digital wallet app and verification of the user's identity, and is applicable to a wide range of payment scenarios.

China's goal is to promote e-CNY as a global payment option, allowing foreign tourists to top up their digital wallets through payments made with Mastercard and Visa cards. This allows them to conduct transactions without having to resort to currency exchange or carry large amounts of cash. In parallel, the intent is also to integrate e-CNY into

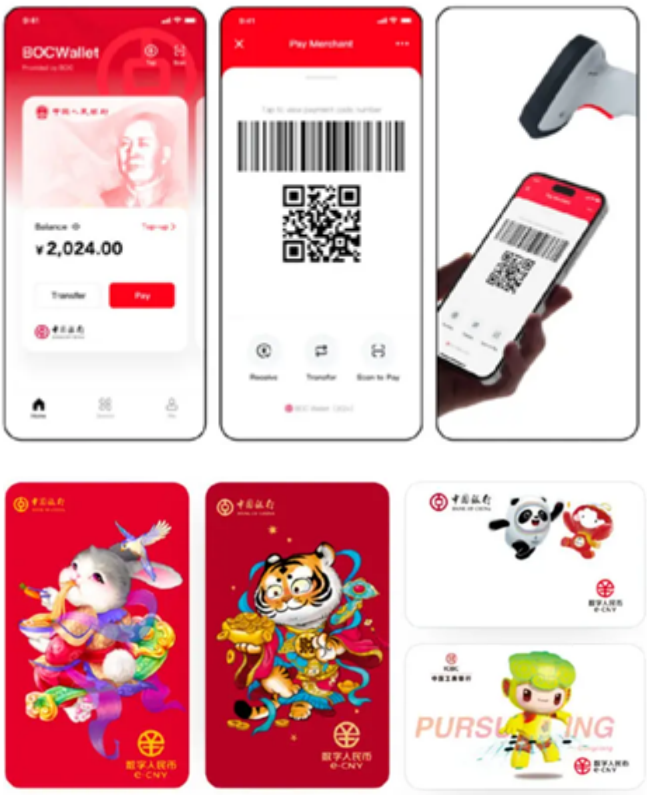


FIGURE 13: e-CNY APP [36]

China's domestic payment system, thus providing a secure and convenient digital solution for Chinese citizens.
The main advantages of the e-CNY app lie in the security ensured through the use of various technologies, such as encryption and digital certificates, the privacy ensured through various levels of anonymity that allow users to make small transactions without having to disclose personal information, and the ease of use, which is inspired by relevant mobile payment platforms such as WeChat Pay and Alipay.

Next Steps

China's financial authorities have invested millions in resources to carry out the development projects of the Digital Renminbi (e-CNY) and currently, the results show clear progress even in comparison with the West. Starting in 2019, when the project of a digital currency really began, until now that we are just a few steps away from seeing a large-scale experimental circulation of the e-CNY (e.g., Project Orchid in collaboration with MAS), a series of events have followed one another that have forced us to review and rethink the structure and architecture of the Chinese digital currency several times. The evolution of projects for the distribution of a Chinese digital currency has led to the distinction between a wholesale distributed currency wCBDC and a retail currency used by the rCBDC population. In this scenario, the People's Bank of China is collaborating synergistically with the Monetary Authority of Singapore (MAS). Singapore's financial authority has announced details of new initiatives to expand its financial cooperation with Chinese authorities, including a cross-border pilot program involving retail use of the latter's central bank digital currency (CBDC)[24].

The Present

Changchun Mu, director of DCI, in the two-day conference of the BIS Innovation Summit 2023 emphasized that:
"We live technological innovation in an era of uncertainty. Together with representatives of the central banks of the United States, Spain and Chile, he spoke on the topic The process of technological innovation in central banks, comparing innovation in the public sector with innovation in the private sector for much of the meeting"[8].
One of the reasons for distinguishing between two types of CBDCs, one retail and the other wholesale as stated during the meeting (BIS) is due to several issues:

- Ledgers (DLTs) are not suitable or for now inefficient to make the process scalable to retail customers, in other words they do not meet the retail requirements for a population as large as China's.
- Linked to the previous point, the problem intensifies when we consider cross-border transactions globally.
- Lack of skills and abilities to manage the processes related to the transmission of payment information.
- The process that combines Offline and Online transactions is not yet well defined;
- The problem of decentralized information. Advanced DLTs are not decentralized because:
  - The management of computer source codes is not self-powered;
  - The organization of network paths;
  - The technological path of the entire DLT gorvernance.

- Another problem is related to the issuance of stablecoins, which are actually issued by centrally managed fintech companies, as well as the associated smart contract as a result.
- Cascading, meaning that all the money flows generated are managed by centralized banks that support a pool of assets governed by algorithms that will be proprietary and therefore subject to risks of transparency and manipulation at multiple levels, starting with prices.
- If everything were decentralized, the problem that would arise later is induced by issues of maintenance and updating of the systems that regulate and incorporate DLTs, and this is not possible automatically. It is necessary to rely on specialized service providers who would provide a centralized service.

Summing up these issues, it all comes down to a discourse of liquidity and market risk for central banks, since all the points mentioned above are connected by the process of decentralization that starts from central banks and is recentralized by financial institutions. According to this approach, some of the supervisory requirements of the supervisory authorities are missing. Central banks, being responsible for the issuance of FIAT currency, its operation and settlement, cannot allow the process to be reduced to centralization to financial institutions. Lacking the requirements that characterize central banks, including that of being a lender of last resort and the PCC to mitigate the risk of default of OTC transactions, the risk is related to trust problems, because DLT is based on Blockchain technology (in the mBridge reference project). The contrast between decentralization and centralized systems emerges when looking at the choice of technology to use to face the global challenge of a multi-CBDC platform and the delicate issue of regulation which must be continuously updated. Central banks must be able to build a regulatory framework with characteristics of flexibility and harmonization between different jurisdictions, capable of simultaneously accommodating technological innovations. The guidelines drawn up by international regulators, various committees and management boards converge towards this type of solution. Alongside this issue Europe has said it is adamant about taking a different position on data protection and privacy through the General Data Protection Regulation (GDPR), while China has stated that one of the purposes of the CBDC is to prevent tax evasion and this means that the authorities will be able to obtain information or data if necessary, therefore it will be appropriate to follow developments also with a view to comparing differences in terms of data and privacy policies that could influence the development of CBDCs.
In other words, the battle for CBDC in the EU [European Union] and the USA [United States of America] is based on privacy in fear of the government comprehensively controlling and understanding the flow of payments. With China's CBDC, the government controls both the processing technology and account holder data, but needs court-issued warrants in case officials want to settle both sides. China has recently introduced data policy laws that are much more stringent than the EU's GDPR and these data laws do not allow the Chinese government to turn to a phone company to investigate an individual, but they need a specific warrant. The Western response of the United States and the Eurozone to this regulatory advancement consists in having created a project for a digital currency model that is able to prevent the government from taking possession of the data and the anonymous storage remaining in the hands of banks or organizations by handing over only the transaction system to governments while maintaining privacy through ledgers.

mBRIDGE Project

The continuous search for interconnections on every socio-cultural aspect and globalization have also transformed the economic and financial system of payments. Today's system of cross-border payments, particularly for CBDCs, calls for increasingly challenging and innovative requirements for the technologies and infrastructures available. Between 2019 and 2020, the G20 launched a global programme, involving the central banks of many countries, to improve the cross-border payments system called mBRIDGE. The result of the cooperation of several countries in projects, including Jasper-Ubin (Bank of Canada and Monetary Authority of Singapore (2019)), Stella (European Central Bank and Bank of Japan (2019)), Aber (Saudi Central Bank and Central Bank of the United Arab Emirates (2020)), Jura (BISIH et al (2021b)) and Dunbar (BISIH et al (2022)), mBRIDGE is the final result that led to converge towards the realization of a joint project between the BIS Innovation Hub Hong Kong Kong Centre (HKC) and four central banks in Southeast Asia and the Middle East: the Hong Kong Monetary Authority (HKMA), the Bank of Thailand (BOT), the Central Bank of the United Arab Emirates (CBUAE), and the Institute for Digital Currency of the People's Bank of China (PBCDCI).
The main feature of mBRIDGE is the identity of a single platform with direct access with MVP features [8] capable of reflecting cross-border multi-CBDC arrangements imposed by central banks to:

1. Efficiency (24/7);
2. Minimum transaction costs;
3. Real time;
4. Scalability.

And (network of direct central bank and commercial participant connectivity and greatly increase the potential for international trade flows and cross-border business at large.) can provide a direct connectivity network between central banks and trading participants and significantly increase the potential of international trade flows and cross-border activities in general.
The prerogatives of central banks remain those of preserving and integrating:

1. Monetary sovereignty;
2. Monetary and financial stability;
3. Policies;
4. Normative;
5. Privacy.

The systems architecture of the DLT-based platform has been totally replaced by a new private and permissioned blockchain developed specifically in a tailored (or custom) way and called the mBridge ledger (mBL) to meet the requirements listed above of central banks and trading participants. The innovation of this project is given by the extreme level of openness to make contributions to the project. It is possible to freely access codes and implementations through specific APIs that guarantee maximum

[8] i.e. able to connect entities not belonging to the central bank. A minimum version of a final product that is delivered immediately to the market. It's typically simple, appealing, and bug-free. The MVP is a version of a product that has only the features needed to remain profitable. It only has the basic functionality. Delivering an MVP to the market allows you to get immediate feedback on the value of the product[17].

flexibility towards revisions and innovation. In addition, it should be considered that in the pilot version of the project, participants will be asked to provide feedback and suggestions through structured questionnaires, to improve the platform based on individual experiences.
"The mBL is a specialized, flexible and scalable implementation for multi-currency cross-border payments. To maximize the accessibility, adaptability, and extensibility of the platform for current and future users, the platform implements a modular design that provides users and developers with a familiar service-oriented architecture. In this approach, the different modules such as payments, foreign exchange, capital management, and compliance are decoupled and modularized to meet the evolving needs of different jurisdictions. This allows participating central banks to validate, adapt and extend functionalities according to their own technical, commercial and regulatory requirements, and aims to support the autonomy of each jurisdiction in the implementation and adoption of the platform"[5].

Features of the Architectural Design

The peculiar features of the architectural design and the mBL Blockchain that govern the platform's functionalities are summarized below.

Network topology
The mBL liaison structure is that central banks are responsible for carrying out validation operations according to the requirements of the protocol consensus. Each of the central banks provides for the inclusion of commercial banks in the same jurisdiction, significantly expanding the interconnection network by offering their customers the opportunity to take advantage of cross-border CBDC services.

Functional architecture
As presented in chapter 3 and chapter 4, we do not review the different functional modules that make up the classic architecture of these types of platforms, so please refer to chapter 3, 4 for more explicit details and we limit ourselves to listing them:

1. Access Level;
2. Application Layer;
3. Data Layer;
4. Blockchain Layer;
5. Basic Service Level.

Consensus Protocol
The mBridge platform is a private and permissioned distributed system, where transaction validation takes place via a central consensus mechanism in DLT platforms. Known consensus mechanisms include proof-of-work and proof-of-stake, but for private and permissioned systems, such as mBridge, there is no need for economic incentives for public validators.
A desirable consensus mechanism must have Byzantine fault tolerance (BFT), i.e., the ability to withstand malfunctioning components that provide conflicting information.
mBridge uses HotStuff+, a variant of HotStuff, which scales linearly with the number of validating nodes, unlike most other BFT protocols that scale quadratically. This allows for greater computational efficiency. Development teams have developed a new dynamic threshold consensus (Dashing) mechanism for permissioned blockchains. Dashing improves efficiency and robustness over HotStuff+ by using triple certificate security, which involves the use of three certificates with different thresholds in different network circumstances. This approach allows for greater efficiency and scalability, especially when there is high transaction concurrency.

Privacy Controls
The design of CBDC platforms must carefully address choices related to privacy, which is not a binary issue between complete anonymity and total disclosure. There are many nuances to consider. For example, in cash transactions, only the parties involved know the existence of the transaction, not the issuer of the currency. However, for transactions of large amounts, such as the transfer of real estate securities, some information about the origin of the funds is often required. The implementation of privacy in mBridge involves the mBridge platform incorporating privacy controls to protect critical transactional data, such as payer and payee identities, the amount, and details of the CBDC. It uses pseudo-anonymous addresses with randomly auto-generated key pairs, ensuring that only the parties involved and their respective central banks can see sensitive transaction details. As example: "In a hypothetical transaction scenario, if a UAE bank makes a payment to a Hong Kong bank in e-HKD on mBridge, the transaction details would only be visible to clearing members and their central banks. Other participants, such as the Bank of Thailand (BOT) and the People's Bank of China (PBCDCI), would not see the details. If the payment was in e-THB, the BOT would also see the details." The need for Privacy Controls is determined by the fact that without these controls, every participant in the mBridge platform could access sensitive transaction details, as all information would be visible on the shared ledger.

Functional Implementations

1. Issuance and redemption. It is planned to define a system that provides for automated or manual integration, capable of also connecting with traditional payment systems, especially with reference to countries or jurisdictions that have not yet adopted a CBDC system or that in any case do not have the provision of integrated APIs:
   (a) Manual Issues and Refunds;
   (b) Automatic Issues and Refunds.
2. Payment and PvP are critically tought divided into two categories:
   (a) Simple, single-currency push payments;
   (b) Dual-currency PvP FX transaction.

Political Considerations

The creation of a common multi-CBDC platform involves various political, legal, and regulatory considerations, given the differences between the monetary and governance systems of the four jurisdictions involved. This made it possible to explore a flexible design that respects the specificities of each jurisdiction, while maintaining common principles that are fundamental to the operation of the platform.

Measures to Preserve Monetary Sovereignty
A crucial issue concerns the protection of central banks' monetary sovereignty, as cross-border access to CBDCs could destabilize national monetary systems, leading to volatile capital flows and currency substitution. To mitigate these risks, the platform must consider whether to allow commercial banks to access CBDCs from other jurisdictions.

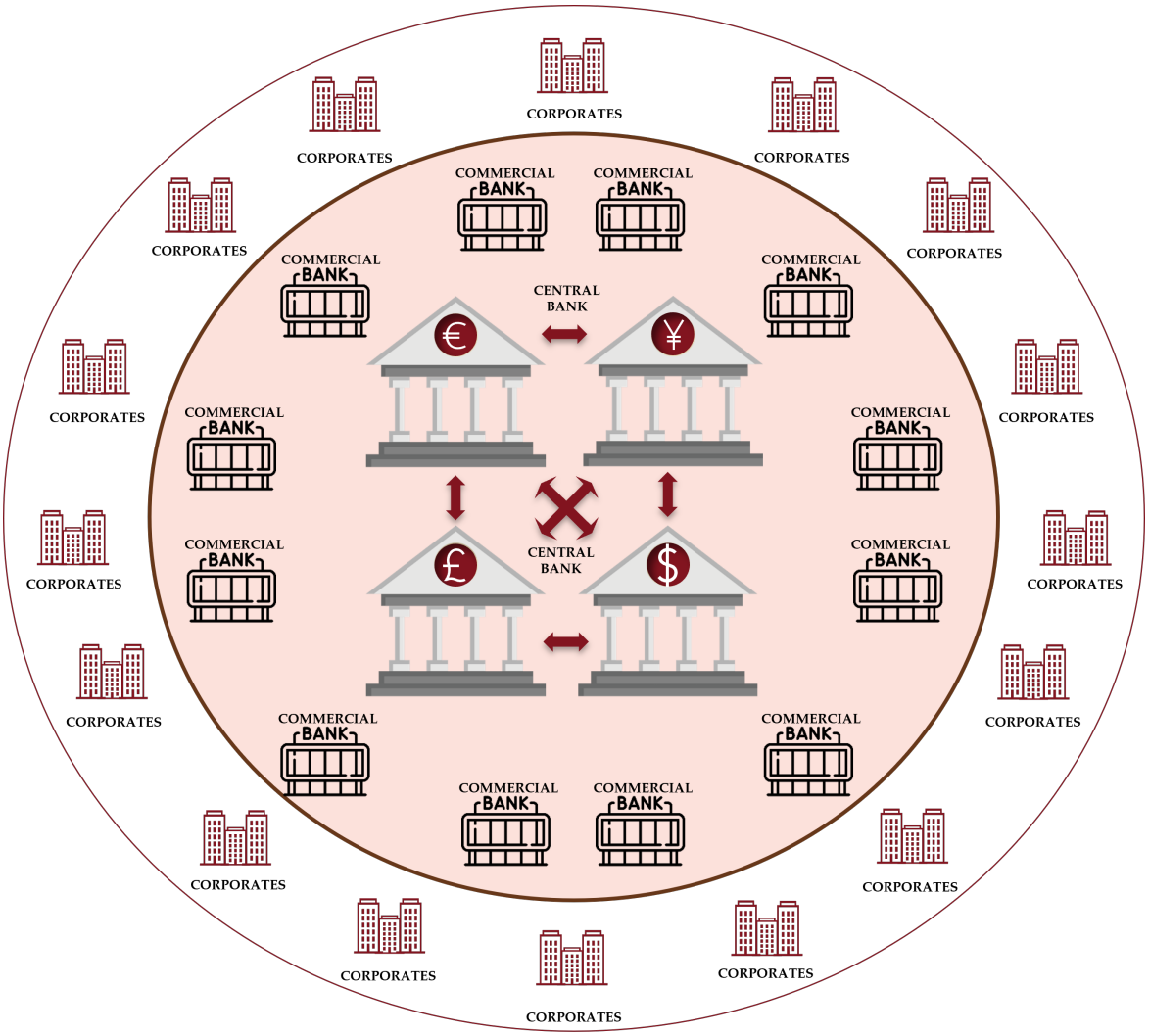


FIGURE 14: mBridge Platform - Network Design

mBridge Platform Project
The mBridge project allows both domestic and foreign banks to hold and operate in CBDCs, facilitating cross-border payments without hampering public policy or central bank capabilities. The platform provides flexible controls on the issuance, redemption, and use of CBDCs to ensure that each jurisdiction's monetary sovereignty is respected, allowing for customization according to local needs.

Pilot Operations
During the mBridge pilot, participating banks were allowed to operate in CBDCs from other jurisdictions, but foreign banks had limitations on the movement of CBDCs. The transactions excluded domestic and cross-border transactions in foreign currencies to ensure that a national bank was always involved, avoiding the accumulation of offshore domestic currency and limiting speculative use. Additional analysis and countermeasures will be required before excluding transactions can be included in future phases.

Data Privacy and Governance
Data privacy and governance are critical to mBridge's success, considering the involvement of several central and commercial banks. During the pilot, sensitive data was stored off-chain and shared only on a necessary basis, protecting users' identities through pseudo-anonymity. However, the pilot's centralization has raised privacy concerns. In the future, a decentralized distribution of data will be explored, where only a few pieces of data are recorded on the blockchain, while sensitive data remains in local, encrypted databases.

Legal and Regulatory Considerations
Legal Categorization of CBDCs can be classified differently (such as currency, representation of funds, debt, etc.) depending on local laws, requiring possible regulatory updates.

Central Banks' Participation
The powers of central banks, focused on the stability and integrity of financial systems, support their participation in mBridge. Regulatory adaptations may be necessary to ensure compliance.

Role of the Platform Operator
The management of the platform can be decentralized, with each participating central bank responsible for specific governance roles. Some core tasks may require a dedicated structure.

AML/CTF/Sanctions Compliance
Participating commercial banks must comply with anti-money laundering, anti-terrorism, and sanctions regulations, with the platform certifying transaction compliance.

Purpose of the Regulation
The settlement of transactions was achieved through legal agreements between central banks and commercial banks, adapted to local regulations.

Privacy Laws
mBridge's pseudo-anonymity and privacy protection features must be adapted to different local data privacy and governance regulations.

Other Legal Considerations
Further analysis of laws regarding contracts, intellectual property, competition, cybersecurity, and dispute resolution is needed for a production-ready system.

Trying the conclusions, while central bank participation in mBridge is generally possible, regulatory adjustments and a robust contractual architecture may be required to ensure legal certainty and regulatory compliance.
On June 5, 2024, a press release by BIS, related to the mBRIDGE project was published. It is stated that a great result has been achieved: the achievement of the minimum viable product stage. Reaching this important stage determines a crucial point since implicitly all the functional requirements to proceed with the extension of the project on a large scale are present. In addition, with a view to collaboration, the works were opened to international participants in order to create synergy.

References

[1] **Azzone, M., and Barucci, E.** *Evaluation of sight deposits and central bank digital currency.* Journal of International Financial Markets, Institutions and Money Vol. 88, October 2023.

[2] **Baosheng Hu.** *The Development and Implementation of the Digital CNY*. Highlights in Business, Economics and Management, January 2024.

[3] **Barucci, E.** *Euro Digitale.* Egea, May 2023.

[4] **Bindseil, U.** *Tiered CBDC and the financial system.* ECB Working Paper Series n. 2351, January 2020.

[5] **BIS** *Project mBridge: Connecting economies through CBDC.* Bank for International Settlements, October 2022.

[6] **Broby, D.** *Central bank digital currencies - Lessons from China*. Journal of Information Science and Engineering, April 2024.

[7] **Caudevilla, O. and Henry, M. K.** *The Digital Yuan and Cross-Border Payments: China's Rollout of Its Central Bank Digital Currency*. University of Hong Kong Faculty of Law, April 2023.

[8] **Changchun, M.** *BIS Innovation Summit 2023: Technological innovation in an age of uncertainty*. Bank for International Settlements, March 2023.

[9] **Chen, Y.** *Introduction of the Postal Savings Bank of China*. 2007.

[10] **Demirguc-Kunt, A. et al.** *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank Publications, 2022.

[11] **Duffie, D. and Economy, E.** *Digital Currencies the US, China,and the World at a Crossroads*. Hoover Institution Press, March 2022.

[12] **European Central Bank.** *Update on the work of the digital euro scheme's Rulebook Development Group*. January 2024.

[13] **Feng, C., and Che, P.** *China's digital yuan: e-CNY wallet tops download charts in Apple and Xiaomi app stores ahead of Lunar New Year*. South China Morning Post, January 2022.

[14] **Fergus, R. and Pascoe, A.** *The role of WeChat Pay and Alipay in DC/EP*. Australian Strategic Policy Institute, 2020.

[15] **Fullerton, E. and Morgan, P.** *The People's Republic of China's Digital Yuan: Its Environment, Design, and Implications*. ADBI Discussion Paper Series, February 2022.

[16] **Gang, Y.** *Yi Gang: Speech Conference of the Bank of Finland Institute for Emerging Economics*. Bank for International Settlements, November 2021.

[17] **Giblin, R., Lindstrom, J. and Kahi, D.** *Envisioning to delivery, PoC,prototypes, pilots and MVP*. BIS Innovation Hub, January 2021.

[18] **Interesse, G.** *China's Digital Yuan App Gets a Boost: New Features Enhance Convenience for Foreign Users.* China Briefing, September 2023.

[19] **Klein, A.** *China's digital payments revolution.* Brookings Institution, 2020.

[20] **Kong, S.** *China's digital yuan transaction average of $265 points to*

business usage. Ledger Insights, July 2023.

[21] **Marr, B.** *Facebook's Blockchain-Based Cryptocurrency Libra: Everything You Need To Know*. Forbes, October 2019.

[22] **Mazzoni, N., and Ciminelli, V., Morisani, G.** *Asset Tokenization: Potential Applications.* Argo n. 25, April 2024.

[23] **Menegon, A., Colombo, G., Mori, G., Mazzoni, N., Bainotti, M., Campaniolo, G., Migliaccio, E., Nava, L., Stabellini, C., and Zanolli, M.** *Digital Euro: Now and Beyond.* Argo Collection n.6, December 2023.

[24] **Menon, R.** *Speech Conference at the Singapore FinTech Festival 2023. "Shaping the Financial Ecosystem of the Future"*. Monetary Authority of Singapore, 2023.

[25] **Mori, G., and Pizzamiglio, F.** *CBDC - Exploring a New Digital World.* Research Paper Series n.55, April 2023.

[26] **NFRA.** *Public Notice of the CBRC No.1*. April 2003.

[27] **PSBC.** *About PSBC*. March 2023.

[28] **Shuzi, R.** *'Digital Renminbi' emerges from theory to reality*. Jingji Cankao Bao (Economic Information Daily), January 2020.

[29] **Sun, L.** *Is the Digital Renminbi 'Violating User Policy' a Misunderstanding? What Is the Design of 'Controllable Anonymity'? Look at the Latest Response from the Central Bank Mu Changchun*. Securities Times, STCN, March 2021.

[30] **Wang, J.** *Inclusion or expulsion: Digital technologies and the new power relations in China's "Internet finance"*. Sage Journals, February 2018.

[31] **Working Group on E-CNY Research and Development of the People's Bank of China.** *Progress of Research & Development of E-CNY in China* PBOC Documents, July 2021.

[32] **World Bank Group, People's Bank of China.** *Toward universal financial inclusion in China: Models, challenges, and global lessons*. World Bank Documents, February 2018.

[33] **Zhang, J.** *How Alibaba powered billions of transactions on Singles'Day with 'zero downtime'*. South China Morning Post, November 2019.

[34] **Xinhua.** *China fast-tracks digital yuan trials for Beijing Winter Olympics*.December 2021.

Sitography

[35] **Agricultural Bank of China.** *Website*.

[36] **GWBMA.** *Website*.

[37] **Hong Kong Interbank Clearing Limited.** *Website*.

[38] **Hong Kong Monetary Authority.** *Website*.

[39] **Worldometers.info.** *Website (China Demographics)*.

[40] **Worldometers.info.** *Website (China GDP)*.

Introducing Sectoral PD Satellite Models through Constrained BACE

About the Authors

Andrea Mauri:
Manager
After taking a PhD in High Energy Theoretical Physics and having spent 10+ years in academic research and teaching, he moved to Risk Management with special focus on Credit Risk area. Currently involved in projects for major italian banks on implementation and performance of periodic EBA, ICAAP and Climate Stress Test exercises; credit risk model development for both regulatory and managerial purposes; methodological development of Credit Risk forecasting tools based on dynamic balance sheet hypothesis. He is also Co-Head of the iason Credit Risk Competence Center.

Raffaele Di Sivo:
Credit Risk Quant
He holds a Bachelor in Banking and Finance and a Master degree in Finance and Risk Management. He obtained a specialisation in Quantitative Finance at Politecnico di Milano. He is currently involved, as a Credit Risk Consultant, on developing a monitoring data quality framework for IFRS9 credit risk parameters at one of the major Italian banks. He has experience in ICAAP, stress testing and climate exercises.

Riccardo Greco:
Credit Risk Quant
He obtained an MSc in Statistical Sciences from the University of Bologna. He began his tenure with iason in May 2023 and, as a Credit Risk Analyst, he has been involved in developing credit risk models for major banking institutions.

Introducing Sectoral PD Satellite Models through Constrained BACE

Andrea Mauri Raffaele Di Sivo Riccardo Greco

In this paper we propose a methodology to estimate sectoral PD Satellite Models that can be consistently used to perform scenario analysis based on sector specific shocks. In particular, we complement the Bayesian averaging estimation approach known as BACE, with a study of the relative importance of the estimators in terms of Dominance Analysis. The final aim is to estimate models with sufficient sensitivity to the sectoral scenario driver, identified with the Gross Value Added (GVA). We end up with a methodology to produce native sectoral PD models, without having to deal with external models overlays and based on an algorithmic and easily maintainable calibration procedure. The faithful representation of the sectoral scenario narrative is managed through a customizable parametrization of the choice of models that are involved in the averaging process. Our methodological set up is particularly suited for any kind of sectoral analysis involving GVA scenarios, for instance in the case of EBA EU-wide and Climate Stress Test exercises.

Sectoral stress testing is an essential component of modern risk management and it is a vital tool used by financial institutions and regulators to assess the resilience of specific sectors of the economy or financial system under adverse conditions. This approach helps in identifying vulnerabilities within particular sectors, enabling stakeholders to implement measures to mitigate potential risks. Unlike traditional stress tests, sectoral stress tests concentrate on the collective performance of entities within a particular sector by introducing sector specific shocks, thus providing a more granular understanding of risks.
During the past few years, scenario analysis based on sectoral shocks have been progressively combined with the standard stress test exercises. There have been two main areas of application that required a specific sectoral analysis: Climate Stress Testing (starting from ECB 2022 bottom-up exercise) and EBA EU-wide Stress Tests (e.g. Covid-19 pandemic projections during 2021 exercise, sectoral scenarios and energy intensive sector classification in 2023). In this context, it is becoming increasingly important to develop statistical tools that are able to fully capture, together with general trend set by macroeconomic variables, the narrative underlining the sectoral nature of the scenarios. This introduces a new layer of complications in model estimation that includes availability of sufficiently granular data, potential lack of sensitivity of the models to the sectoral drivers, need of flexibility in the methodology to meet the different use cases and efficient model design in order to produce a set-up that can be consistently maintained.
In this paper we address the problem of sectoral scenario analysis by focusing on credit risk parameters and considering the case of estimation of PD satellite models. The main approaches currently used to introduce sectoral differentiation into PD satellite models can be essentially summarized into two main categories:

- **Overlay models**: non-sectoral models are first developed, leveraging on standard macroeconomic explanatory variables. Sectoral differentiation is introduced as an overlay coming from a second set of independent models, that produces corrections to be applied on top of the main non-sectoral impacts.
- **Native sectoral models**: models directly depend on sectoral explanatory variables together with other macroeconomic drivers and are thus able to perform sectoral scenario analysis without the introduction of further add-ons.

The two approaches can be practically introduced with a vast spectrum of variants, but generally speaking we can identify some common advantages/disadvantages. Overlay models usually provide a better control on the general trend of the macro scenario and the intensity of the overlays can be calibrated to produce a faithful representation of the sectoral narrative. As a drawback, this approach introduces two set of independent models, making it difficult to justify their methodological coherence and giving rise to a framework that is more cumbersome to be maintained. Native sectoral models overcome possible methodological inconsistencies due to the presence of multiple models and since they rely on a unique framework are naturally easier to be maintained. On the other hand, in this case it may be more difficult to estimate models whose sensitivity properly capture the sectoral drivers, giving rise potentially to a poor sectoral differentiation.
In this paper we introduce a methodology to estimate sectoral PD Satellite model following the native sectoral modeling approach discussed above. In particular we refer to the Bayesian estimation approach known as BACE, where one samples the model space and takes an average projection weighting the sampled models in terms of a penalized likelihood [4]. This approach has several advantages with respect to other methodologies (for a critical review see [9]) and has already been applied for the estimation of PD and LGD Satellite Models implemented in iason proprietary solution *G-RiskPar* [8] [10] [11].
Since we would like to apply the methodology to perform sectoral scenario analysis, we complement the original modeling approach with a study of the relative importance of the estimators in terms of Dominance Analysis (for

a review see [1]). The final aim is to estimate models with sufficient sensitivity to the sectoral scenario driver, identified with the Gross Value Added (GVA). We end up with a methodology to produce native sectoral PD models, without having to deal with external models overlays and based on an algorithmic and easily maintainable calibration procedure. The faithful representation of the sectoral scenario narrative is managed through a customizable parametrization of the choice of models that are involved in the averaging process.
Our methodological set-up is particularly suited for any kind of sectoral analysis involving GVA scenarios, for instance in the case of EBA EU-wide and Climate Stress Test exercises. A dedicated discussion is needed for the case of climate stress testing, since the regulator requires the introduction of information also at level of single counterparties [5]. Models in a climate stress test capture two main type of impacts:

- **Indirect impacts:** models that transmit climate shocks to parameters through climate-related macroeconomic variables (e.g., RRE, CRE, and GVA) connected to the sector relevant to the counterparty.
- **Direct impacts:** Models that utilize specific variables (e.g., energy consumption, water consumption, GHG emissions, carbon price, Carbon/GHG emissions intensity, EPC labels), referred to as climate-related transition variables.

From a methodological standpoint, direct impact models are more precise and accurate in determining the climate shock, but they are extremely complex to implement as they require a highly granular and detailed database for each counterparty. Conversely, while indirect impact models are easier to implement, relying on the simple introduction of a macroeconomic variable into the pool of classical regressors, they suffer from limitations in transmitting shocks. It is important to stress that our approach can be consistently used to capture the indirect impact of climate scenarios, whereas direct impact inevitably needs an analysis at the level of single counterparties which is outside the scope of this paper.
The paper is organized as follows. We start with a brief methodological introduction in Section , reviewing the main aspects of BACE methodology and Dominance Analysis. In Section we provide details on the calibration process, including information on input data sources and final models granularity. In Section , we discuss in details the role of the dominance threshold and use our models to simulate an EBA-like stress exercise. Final considerations can be found in Section .

Methodological Overview

As already mentioned in the Introduction, the main issue with methodologies based on native sectoral models is given by the fact that the models combine sector specific macroeconomic variables with traditional macrovariables, risking insufficient explanation of default probability trends by the former, as most variability might be captured by other macroeconomic factors. This issue is further pronounced in a Bayesian model averaging approach, where algorithmic selection naturally assigns greater weight to variables that provide more explanatory power, thereby marginalizing variables that do not significantly explain the variability of the dependent variable. In order to describe how we tackle this problem, it is necessary first to explain how the BACE methodology works and then to outline the constraints introduced to ensure that sectoral variables play a decisive role, thereby addressing the problem of the explanatory power of individual variables on the predictive capacity of the model. They key contact between the BACE methodology and the Dominance Analysis (DA) will be deeply investigated.

BACE Estimation Approach: a Quick Review

The BACE methodology was firstly introduced by Doppheffeler, Miller e Sala-i-Martin [4]. In the context of Satellite Models estimation, we developed a proprietary algorithm [11] based on three main steps that we review here, with a central focus on BACE methodology. Briefly, the purpose of the algorithm is to avoid expert judgement, often used to estimate satellite models, aiming to preserve a statistically sound model selection phase. Moreover, the algorithmic nature of the model estimation and model selection processes allows to consistently estimate a large number of models, thus addressing the increasing need for more granular risk identification. The algorithm schematically operates as follows:

For each counterparty type, a list of relevant macroeconomic explanatory variable is identified. The expected impact of each macro variable on the PD (in terms of economic sign) is also determined, leading to a final list of N independent variables together with (possible) constraints on the signs.

A total of M OLS regression models are estimated by considering all possible combinations of k independent regressors, chosen from our initial pool of N macrovariables. Hence:

$$M = \sum_{k=1}^{K} \frac{N!}{(N-k)!k!}. \tag{1}$$

After excluding certain models based on the assumptions we made in the step **A)** and by leveraging on statistical criteria, the core of the BACE methodology is applied by averaging model coefficients using weights proportional to the posterior distribution of each individual model, having the following functional form:

$$P(M_j \mid y) = \frac{P(M_j) T^{-k_j/2} \mathrm{RSS}_j^{-T_j/2}}{\sum_{i=1}^{M} P(M_i) T^{-k_i/2} \mathrm{RSS}_i^{-T_i/2}}, \tag{2}$$

where M_j identifies the j-th model with $j \in [1, M]$, y is the the dependent variable vector, $P(M_j)$ is the prior probability of the j-th model, T_j is the number of observation used for the j-th model, k_j is the number of independent variables, and finally RRS_j identifies the Residual Sum of Squares of the j-th model. A distinctive feature of BACE methodology is that, unlike classical Bayesian-averaged models, the *a priori* probability weight of the j-th model is fixed as uniform ($\frac{k}{N}$) and thus cancels out from Equation (2) and the models is free of its weight. After the posterior probability is computed, it is used to estimate the posterior coefficient for each single variable involved in the modelling phase:

$$E(\beta_i|y) = \sum_{j=1}^{M} P(M_j|y)\hat{\beta}_{i,j}, \tag{3}$$

where $\hat{\beta}_{i,j}$ is the i-th OLS estimation of the j-th model and $j \in J_M$ where J_M is M subset composed by those models where the i-th estimate is present. From Equation (2) and fixing the *a priori* probability as uniform, we can deduce that the posterior probability is a useful metric for understanding the explanatory power of a variable within the model. The greater the weight we give to an estimated coefficient, the larger its impact in explaining the variability of the final model.

C-BACE: Dominance Analysis Constraint

Dominance Analysis (DA) is a method used in multiple regression to compare the relative importance of predictors by examining all possible subset models that could be obtained with a different combination of the same regressors [1]. This approach helps in understanding how different predictors contribute to the prediction of the independent variable, providing a detailed view of predictors importance. In general, when discussing DA, one can usually refer to:

- *Complete Dominance*: a predictor X_i completely dominates another predictor X_j (with $i \neq j$) if X_i adds more unique variance than X_j across all subset models. This means X_i consistently shows higher importance in every possible model where both predictors are included.
- *Conditional Dominance*: a predictor X_i conditionally dominates another predictor X_j (with $i \neq j$) if X_i has a greater average additional contribution to the model fit compared to X_j within each subset size. Conditional dominance is assessed by comparing predictors within models of the same size.
- *General Dominance*: a predictor X_i generally dominates another predictor X_j (with $i \neq j$) if the average additional contribution of X_i across all subset models is greater than that of X_j. This measure averages the importance of X_i over all possible models.

In this research, we use the conditional dominance approach to calculate the relative importance percentages of the regressors involved in the BACE estimation process. The following steps are followed:

1. *Fit All Subset Models*: generate all possible subset models of the predictors. For k predictors, this involves fitting 2^k models;
2. *Calculate R^2 Values*: for each subset model, compute the proportion of variance in the criterion variable Y explained by the predictors in the model (R^2);
3. *Compute Additional Contributions*: for each predictor, calculate its additional contribution to R^2 by comparing models that include the predictor to those that do not;
4. *Averaging Contributions*: calculate the average additional contribution for each predictor within each subset size;
5. *Relative Importance*: The relative importance percentage for each predictor can be derived by comparing their contributions. For instance if predictor X_i has a general dominance measure of 0.30 and the total R^2 for the full model is 0.60, then the relative importance of X_i is $\frac{0.30}{0.60} \times 100 = 50\%$.

In order to let the posterior probability be a good proxy of the weight that the variable has in the final model, it must be calculated over the entire pool of models that are subject to averaging. At this level, constraints can be applied on the pool of models as already mentioned in the previous Section at Step **C)**. In particular, our algorithm excludes from the calculation of the Bayesian mean all those models that display wrong economical signs (e.g. a positive sign for GDP for PD models) and are not statistically consistent (e.g. violate OLS assumptions).
At this stage, we introduce a new step (between B and C) within the above algorithm, specifying more about the models that will have to feed BACE:

For each of the j-th estimated models a conditional DA is performed, which estimates a relative importance index for each variable in the estimated model. Only those models that contain a GVA with a relative percentage importance greater than a given cut-off will feed into the final pool of models on which to average. Therefore, we end up with a methodological approach that depends only on two hyperparameters, that the user can choose to calibrate:

- The **number *k*** of regressors contained into each OLS models. This should be related to the depth of the independent variable time series, in order to avoid overfitting;
- The **cutoff *z***, that we use to identify models for which the added value can significantly explain the variability of the model. It should be set in such a way as to balance the sensitivity with respect to value added and the possible drop of performance in terms of R^2 of the final model.

Model Calibration

We now apply the methodological framework described in Section to estimate PD sectoral satellite models. We start by introducing details about the input data for model calibration, for both target and explanatory variables (see sections and respectively). We also specify the choice made for the free hyperparameters of the methodology in section .

Target Variables

As a proxy for modeling PDs, we use decay rates time series provided by Bank of Italy[9]. In particular, we select two counterparty types for which sectoral decomposition is relevant, namely Italian Non Financial Corporates (NFC) and Italian Producer Households (HP). The time series span quarterly from 2000q4 to 2022q4 and we estimate models with both geographical and sectoral breakdown (for the full list of models implemented in our solution see Appendix). As a technical note, the target time series have been transformed by logit function to avoid domain issues. In this paper, we choose to illustrate our results by considering examples for the full italian geography without further breakdown and for the "Manufacture of basic metals" (C24-C25) NACE sector. At first, we use the NFC model to conduct a sensitivity analysis on the GVA variable in order to capture the effect of an increasing dominance cutoff z. Secondly, we use the HP model of the same industry sector as en example to analyze the impact of a predefined macroeconomic scenario on the PDs, by simulating an EBA-like stress exercise. The above models are chosen among the full list of estimated models of Appendix , because the general pattern under DA threshold variations is particularly manifest, making them good examples for illustrative purpose.

Set of Macrovariables

The explanatory variables involved in the estimation of PD satellite models are selected on the basis of the available literature on the topic [7][3]. We source the data from publicly available standard data providers (Istat, Banca d'Italia, European Central Bank, Euribor). In particular, we leverage on the following set of independent variables:

[9] Banca d'Italia - Base dati statistica.

cona	co10	co30	co40	co50
0.066%	1.267%	1.828%	2.054%	3.339%

TABLE 5: Sector C24-C25, yearly estimated sensitivity projections under different DA cutoffs

cona	co10	co30	co40	co50
0.054%	0.824%	1.538%	2.154%	3.157%

TABLE 6: Sector averaged italian NFC models sensitivities under different DA cutoffs

cona	co10	co30	co40	co50
89.187%	88.445%	87.629%	87.322%	87.283%

TABLE 7: Sector C24-C25 NFC, R^2 values under different DA cutoffs

cona	co10	co30	co40	co50
76.661%	75.135%	72.160%	70.201%	69.539%

TABLE 8: Italian NFC models, averaged R^2 values under different DA cutoffs

- *Classical macrovariables*: Gross Domestic Product (GDP), 10year-bond, brent oil price, unemployment rate, EUR FX, FTSE MIB Index, house price index, italian-german spread;
- *Sectoral drivers*: gross value added for each NACE sector. It represents the share of GDP produced by the sector to which the GVA belongs.

Each regressor is a quarterly time series and it is considered with 0, 1, 2 and 3 lags. In order to ensure the stationarity of regressors, avoiding the case of spurious regression, we transformed the macrovariables using the quarterly annual variation formula:

$$y_t = \sum_{i=1}^{4} \frac{x_t - x_{t-i}}{x_t}. \tag{4}$$

Model Estimation

After input data elaboration, we estimate the models following the methodological steps that have been fully detailed in Section . As already mentioned, the methodology depends on two customizable hyperparameters, that we set as follows:

- *Cutoff k*: compatibly with the length of input time series, we choose to set k equals to 5 for NFC and a k equals to 6 for the HP targets;
- *Cutoff z*: in order to fully capture the effect of this parameter, we decide to compare the results for a span of different values (no-cutoff, 0.1, 0.3, 0.4, 0.5).

We end up with a total of 261 PD satellite models for the NFC and HP counterparties, differentiated by NACE sector and geography as reported in Appendix .

Case Study

In this Section we use the models selected in Section as examples to test our methodology from different perspectives. Since the DA threshold parameter z plays a central role in our construction, in Section we first study the effect of its variation on the final models GVA sensitivity and on the overall performance. In Section , we finally test the model application to a full EBA-like scenario, highlighting the effect of different DA cutoff choices.

Comparison of Models Estimation with Progressive Dominance Threshold

We perform a sensitivity analysis on the GVA over a three year projection scenario (2023-2025) based on the following assumptions: we keep all the macrovariables fixed to the starting date value except for the GVA, for which we consider a first scenario with baseline variations (BL) over the three years and a second scenario (stressed scenario, ST) with an Year-on-Year one percentage change (-Δ1%) of the GVA with respect to the baseline (BL). This allows to isolate the specific sectoral GVA effect on the forecasts, subject to progressive DA cutoffs.
The sensitivity analysis is performed at first for the "Manufacture of basic metals" sector (NACE ID: C24-C25) beloging to NFC counterparties. Macrovariables values at reference date (2022q4) are taken from actual data from the Economic Bulletin No. 4, 2023 by the Bank of Italy (BoI) [2].
In Table 5 we report the annualized sensitivities (S), given as relative variations of the PDs of the stressed scenario with respect to the baseline, that we choose to compute for the last year of projection (2025):

$$S(t) = \frac{PD_{ST}(t)}{PD_{BL}(t)} - 1. \tag{5}$$

The tabulated data reveal a clear increase in the sensitivity by increasing the DA cutoff.
As highlighted in the Table 6, the same pattern-like feature is observed by calculating the average sensitivity across all the NACE sectors on the full list of NFC models of Appendix .
This finding is not unexpected, given the direct relation between the relative importance of regressors and the value of the final model coefficients. Indeed, variables with higher relative importance translate into a higher absolute value of the variables' coefficients, influencing the explanation of the data variability. Therefore, the final estimates of the

	Unemployment Rate	GVA C24-25	House Price Index
2023	6.00%	1.10%	3.60%
2024	4.00%	1.30%	1.70%
2025	4.50%	1.30%	1.00%

TABLE 9: Baseline Scenario. Unemployment rates are expressed as levels while GVA and HPI scenarios are provided as year-on-year variations

	Unemployment Rate	GVA C24-25	House Price Index
2023	9.00%	-4.90%	-3.50%
2024	12.00%	-12.40%	-3.10%
2025	14.00%	1.40%	-2.50%

TABLE 10: Adverse Scenario. Unemployment rates are expressed as levels while GVA and HPI scenarios are provided as year-on-year variations

	cona	co10	co30	co40	co50
2023	3.440%	3.040%	4.819%	4.015%	0.132%
2024	23.335%	22.186%	21.731%	16.058%	2.523%
2025	50.486%	42.867%	34.537%	24.354%	5.016%

TABLE 11: Sector C24-C25 HP, Baseline-Adverse discriminatory power projections under different DA cutoffs

BACE coefficients are affected both in the posterior probabilities of the model and in the value of the estimated coefficients.
It is important to understand how the different DA thresholds impact the performance of the models. We use R^2 to quantify goodness of fit and report the results for the C24-C25 sector model under different cutoff values in Table 7. As manifest in this Table, in general the model performance slightly decreases as the Dominance threshold is increased. This behavior can be explained in terms of the bias introduced in the coefficients' estimates by the threshold. Hence, the cut-off must be calibrated considering the trade-off between an increasing sensitivity to GVA scenario variations and a deterioration in the overall model fit.

The same decreasing pattern for the performance is present for all the NFC models, as shown in Table 8. For each specific cutoff, the displayed R^2 values are calculated by averaging the R^2 values over the full set of sectoral models.

Scenario Analysis on EBA like Stress Exercise

In the previous section a sensitivity analysis with respect to the sectoral driver (GVA) has been performed. We would like now to test our models against a fully fledged three years macroscenario, to analyze the effects of the Dominance procedure on a real-case stress test simulation.

	cona	co10	co30	co40	co50
2023	3.875%	2.655%	1.574%	1.212%	0.879%
2024	43.175%	37.563%	22.611%	13.118%	1.202%
2025	92.538%	90.231%	46.273%	21.811%	2.782%

TABLE 12: Italian HP models, sector averaged discriminatory power projections under different DA cutoffs

cona	co10	co30	co40	co50
62.03%	60.07%	58.30%	55.83%	54.11%

TABLE 13: Sector C24-C25, R^2 values under different DA cutoffs

cona	co10	co30	co40	co50
61.07%	59.56%	56.36%	55.80%	54.13%

TABLE 14: *Italian HP models, averaged R^2 values under different DA cutoffs*

For this exercise, the BL scenario is provided by the Economic Bulletin No. 4 of the BoI [2], whereas the Adverse scenario is partially derived from the EBA 2023 Stress Test Exercise [6]. Some relevant variables for the Baseline scenario are reported in Table 9, while the corresponding Adverse scenario variables are reported in Table 10. In particular, the sectoral evolution driver (GVA) is precisely taken from the EBA 2023 Stress Test Exercise input shocks [6].
As mentioned in Section , the model for italian HP counterparties and industrial sector "Manufacture of basic metals" sector (C24-C25), is used as a benchmark to process the full scenario. Once again, in analogy with Equation 5, we compute the Adverse vs Baseline PDs relative variations and report them in Table 11. From this Table, it is apparent that the discriminating power between adverse and baseline scenario of the models decreases with the increase of the cutoff. This pattern is due to the fact that in general for increasing DA thresholds, while the added value coefficient is forced to be more important in the model variance explainability, the overall sensitivity to the other explanatory variable is is progressively dumped. Consequently, the stress levels in the final projections will shift from the low-cutoff to the high-cutoff condition, where only the sectoral added value variable exhibit a significant influence.
Again, the same pattern is replicated for the whole set of HP models. Table 12 shows the overall year-by-year/cutoff discriminatory power between *baseline* and *adverse* scenarios averaged over all the sectors. From this analysis, it is clear that too high values for DA threshold can badly affect the out of sample behaviour of the model and the calibration of the parameter must yield sufficient discriminatory power to the final model.
For completeness, we replicate here the performance test of the previous Section for the C24-C25 model (Table 13) and for the sector averaged HP models (Table 14).
The behaviour for the performance indicator is in line with the one displayed for the Non Financial Corporate models introduced in the previous Section and display the same decreasing pattern with increasing cutoff values.

Conclusions

In this paper we introduced a framework to estimate sectoral PD satellite models, based on a native sectoral methodology that combines Bayesian averaging with Dominance Analysis. The main advantage of the methodology resides in its algorithmic nature, that allows for automatic estimation and model selection procedures governed by two customizable hyperparameters. In particular, the practitioner can calibrate manually model sensitivity to selected drivers, introducing domain expert consideration in such a way as to preserve a statistically sound estimation procedure and avoiding the manual choice of a single model out of all the possible consistent candidates. The final models display a good trade-off between performance and sectoral sensitivity, making them particularly suited for Stress Test Exercises driven by GVA scenarios. It would be interesting to extend the analysis of this paper by considering other sectoral drivers, with the definition of an automatic multi-cutoff calibration procedure.

References

[1] **Azan, R. and Budescu, D.V.** *The Dominance Analysis Approach for Comparing Predictors in Multiple Regression*. Psychological Methods, June 2003.

[2] **Banca D'Italia.** *Economic Bulletin Number 4.* October 2023.

[3] **Dees, S., Henry, J. and Martin, R.** *STAMP€: Stress-Test Analytics for Macroprudential Purposes in the euro area*. ECB Research and Publications, 2017.

[4] **Doppelhofer, G., Miller, R.I. and Sala-i-Martin, X.** *Determinants of long-term growth: A Bayesian averaging of classical estimates (BACE) approach.* American Economic Review, Vol. 94, Issue n.4. 2004.

[5] **European Central Bank.** *ECB report on good practices for climate stress testing*. 2022.

[6] **European Central Bank.** *2023 stress test of euro area banks.* July 2023.

[7] **Figlewski, Frydman, H. and Liang, W.** *Modeling the effect of macroeconomic factors on corporate default and credit rating transitions*International Review of Economics & Finance, Vol. 21, n. 1, 2012.

[8] **Mauri, A., Di Sivo, R., Veksin, E.** *LGD Stress Testing: a Bayesian Averaging Modeling Approach*. Research Paper Series, Issue n. 60, Sep 2023.

[9] **Mauri, A., Rubicondo, D., Ferretti, T., Polino N. and Rogante, N.** *Advancements in Bank Stress Tests: from Bayesian Averaging to Causal AI*. Research Paper Series, Issue n. 53, March 2023.

[10] **Scaravaggi, A. and Stucchi,E.** *A Benchmark Framework for IFRS9 Multiyear-PD Curves Estimation and Stress Testing Exercise: an Application*. Research Paper Series, Issue n. 14, April 2019.

Sitography

[11] **Iason ltd.** *Current solutions' portfolio.*

Annex

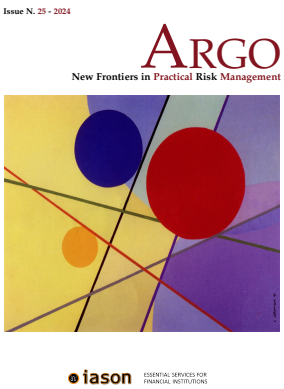
Full List of Models

We describe here the granularity of our full set of PD models for the NFC and HP counterparties. At level of industry breakdown, we have considered the list of NACE sectors reported in Table 15.
At level of geographical breakdown, we estimate the Italian national model; five macro-areas models (North-western Italy, North-eastern Italy, Central Italy, Southern Italy, Insular Italy); twenty Italian regions models.

NACE Sectors
Accommodation and food service activities
Administrative and support service activities
Air transport
Construction
Crop and animal production, hunting and related service activities
Electricity, gas, steam and air conditioning supply
Financial and insurance activities
Forestry and logging
Land transport and transport via pipelines
Manufacture of basic metals
Manufacture of basic pharmaceutical products and pharmaceutical preparations
Manufacture of chemicals and chemical products
Manufacture of computer, electronic and optical products
Manufacture of food products, beverages and tobacco products
Manufacture of furniture
Manufacture of motor vehicles, trailers and semi-trailers
Manufacture of other non-metallic mineral products
Manufacture of textiles
Mining and quarrying
Other sectors net of U
Professional, scientific and technical activities
Real estate activities
Telecommunications
Warehousing and support activities for transportation
Water collection, treatment and supply
Water transport
Wholesale and retail trade and repair of motor vehicles and motorcycles

TABLE 15: *NACE sector list*

In the previous issue



Issue N. 25 - 2024

ENVIRONMENTAL, SOCIAL, AND GOVERNANCE RISKS

EBA Report on the Role of Environmental and Social Risks in the Prudential Framework

TECHNOLOGY

Artificial Intelligence: Risks and Opportunities for the Banking System

Asset Tokenization: Potential Applications

Last issues are available at www.iasonltd.com/research/argo/