sciendo

UDC: 004.89:336.711
DOI: 10.2478/jcbtp-2024-0021

Journal of Central Banking Theory and Practice, 2024, 3, pp. 5-42
Received: 25 December 2023; accepted: 01 March 2024

Milena Vučinić**, Radoica Luburić**

** Central Bank of Montenegro, Podgorica, Montenegro*

E-mail: milena.vucinic@cbcg.me

*** Central Bank of Montenegro, Podgorica, Montenegro*

E-mail: radoica.luburic@cbcg.me

Artificial Intelligence, Fintech and Challenges to Central Banks

Abstract: Technological development particularly boosted by artificial intelligence (AI) has substantial potential to transform many aspects of human lives and the way doing businesses. On the one side, it can offer opportunities, while on the other brings challenges and increases risks. Financial industry is considered the largest user of digital technologies and provider of innovative services. Therefore, it is strongly influenced by digital transformation and under constant threat of cyberattacks. In this paper, the authors are researching the opportunities and risks stemming from the application of AI and its macroeconomic and financial system impacts. The special attention is given to the challenges posed by financial technological development and AI to central banks as they have to adopt to the novel times dominated by electronic financial services and AI tools while at the same time stay persistently dedicated to achieving their key objectives of safeguarding monetary and financial stability as well as contributing to the stability of economic growth. Additionally, the invention of generative artificial intelligence (GenAI) has significantly influenced processes throughout numerous industries, including the financial sector, due to the ability to imitate human behaviour which has enabled computers to behave like humans. Hence, it is important to develop human-centric innovations where AI tools create benefits and serve people instead of replacing them. AI can deteriorate overall inequality so policymakers should act towards developing policies that will ensure AI is used for the good of people and provide benefits for them. The authors further draw attention to the necessity of adopting a robust regulatory framework and building strong and resilient institutions with developed systems for prevention of ever raising cyberattacks.

Keywords: artificial intelligence, central banks, fintech, challenges, opportunities and threats, cyber risk.

JEL Classification: E58, F65, G28, O32, O33.

1. Introduction

We live in a time of dramatic acceleration of changes and unprecedented technological development, in the so-called VUCA (Volatility, Uncertainty, Complexity and Ambiguity) environment. The question is: Are we ready to keep pace with this speed of technological deployment? Trends and market requirements are changing rapidly. This calls for fast and effective actions. Innovative solutions are necessary but they have to be approached carefully, with benefits and consequences examined beforehand. Digitalization is affecting society and economy as a whole thereby posing significant challenges for policy makers. We have been witnessing an accelerated development and widespread use of financial technology, popularly called FinTech, and exponential growth of artificial intelligence (AI) usage.

In regards to innovation, AI is probably the most powerful and influential. Application of AI in industries, including the financial industry, as well as in everyday activities can create advantages but also carry certain risks. Robots, self-driving cars, smart home devices, among others, are changing the way we live and work so the potential problem is what to do if they take over many of the usual activities. AI has potential to increase productivity, boost economic growth, enhance financial inclusion and provide unprecedented use of data in terms of scale, speed and granularity. However, it can also build up risks although the actual dimension of risks it can produce is still uncertain due to widespread usage and extraordinary pace of AI growth. Hence, the risks will depend on the level of technology development and vary substantially among countries. Advanced countries are in a better position to invest in innovative solutions compared to less developed economies, which will generate further disparities among countries. Accordingly, as a result of greater application of AI, advanced economies can be exposed to more risks stemming from AI as well. Although risks of AI are numerous, cyber risks are considered the most critical and powerful. Other risks include, but are not limited to data security and privacy issues, lack of transparency and explainability, rising inequality due to lack of necessary skills of employees, potential for increasing unemployment and job losses. As financial industry is considered the biggest user of digital technologies and provider of innovative services, it is highly exposed to cyber threats. Therefore, the society needs future-proof institutions supported with robust regulatory frameworks in order to respond to new-era challenges led by innovations, particularly generative artificial intelligence (GenAI) due to its ability to mimic human behaviour and produce new results using enormous available unstructured data.

Digital transformation should help people improve business processes and raise productivity, but combined with AI it can lift up possibilities by trying to make computers think and act like humans. Still, what is crucial is to keep humans in the centre. Implementation of new technologies, particularly GenAI, should complement people at work instead of being substitute for them.

Application of technology is transforming the world of finance. Innovation-led benefits include, inter alia, enhanced market competition, increased efficiency, faster financial services at lower cost, and greater financial inclusion. These benefits are accompanied by risks whereas customer privacy issues and cyber threats stand out. Fintech has potential to influence financial stability through expansion of cryptocurrencies, stablecoins and crypto assets which may further jeopardize traditional use of central bank money and bank deposits. Here is to emphasize the importance of central banks whose role has been challenged lately especially due to expansion of unsupervised fintech firms that have started to use AI technology and tools.

Central banks are directly impacted by AI. Without questioning the achievements of their key objectives including maintaining monetary and financial stability as well as contributing to sustainable economic growth, central banks have to adopt to new market trends and requirements. The latter requires developing adequate regulations, strengthening and modernizing supervision methods, building digital infrastructure and ensuring strong cyber-resistant institutions that can cope with new challenges arising from the use of digital technologies. It is very important to nurture the culture of change and build the atmosphere in organizations where both management and employees are ready to embrace changes and benefit from them. That requires investment in education and reskilling of existing workforce as well as employment of new, already skilled people. In the era of AI, it is crucial to prevent job losses and growing unemployment. Still, tendencies are not very promising as far as AI exponentially grows while its widespread use and automation are taking toll on the job market.

The paper consists of five sections. After a brief introduction, in the second section authors describe evolution of AI. The third section is dedicated to the impacts of AI in terms of opportunities and threats through selected macroeconomic and financial system channels including productivity, labour market, monetary policy, financial stability, payment system oversight, anti-money laundering, data usage, and cyber security. The fourth section discusses financial technology developments in the light of AI and challenges posed to central banks. Finally, the paper ends with concluding remarks.

2. AI Evolution

"The potential benefits of creating artificial intelligence are huge…Every aspect of our lives will be transformed. In short, success in creating AI could be the biggest event in the history of our civilization. But it could also be the last, unless we learn how to avoid the risks….In short, the rise of powerful AI will be either the best, or the worst thing ever to happen to humanity. We do not yet know which." – these are powerful words of the distinguished professor Stephen Hawking during his speech at the launch of the Leverhulme Centre for the Future of Intelligence (Hawking, 2016).

ISO/IEC 23053:2022, Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML), defines artificial intelligence as „engineered systems that generate outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives" whereas "ML is a branch of AI that employs computational techniques to enable systems to learn from data or experiences". AI includes an extensive array of technologies that reflect diverse approaches to dealing with mentioned complex problems.

AI has evolved over time. In that regards, three categories can be distinguished. Those are: "Early" artificial intelligence, Machine learning and Generative AI models (Liang, 2024). "Early" artificial intelligence refers to rule-based models or systems that solve problems by exact rules applied to a defined set of variables. For example, asking a question that leads to pre-defined follow-up questions. Internal loss forecasting models or early algorithmic trading, might be considered forms of early artificial intelligence. These tools have been applied in finance so far.

Machine learning, unlike rules-based systems, detects relationships between variables without explicit instruction or programming while data are the key input and the system identifies patterns from the data (Liang, 2024). By providing feedback to the system, machine learning model can learn to do better in the future. Machine learning has widespread use in the financial sector and a good example of that is its usage for fraud detection tools.

Neural networks are considered probably the most significant technique in machine learning whereas their main building blocks are artificial neurons that take multiple input values and transform them in a non-linear way to produce a single number – like logistic regressions (Araujo, Doerr, Gambacorta, and Tissot, 2024). As Araujo et al. argue, alike human brain neurons, the output value of artificial neurons is equivalent to an electrical impulse transmitted to other neurons whereas the artificial neurons are ordered in a sequence of layers and a network's

depth depends on the number of layers. Constant and weights of neurons are attached to the output of previous layers' neurons and are called parameters that define the strength of connections across neurons and layers. As parameters develop through iterative training, deeper networks with more parameters entail more training data but also produce higher quality forecast. Also, neural networks are behind face recognition or voice assistants in mobile phones. Further developments revealed transformers, which considerably enhanced the performance of neural networks in natural language processing (NLP) and empowered developments of large language models (LLMs) that are neural networks trained to predict the next word in a given sequence of text, and to do that, LLMs learn to absorb all the written knowledge on which they were trained. Doerr, Gambacorta, and Serena (2021) point out that Natural Language Processing refers to a common set of applications of machine learning used to excerpt information from written texts. The emergence of large language models (LLMs) has exceled putting GenAI into popular discourse, linking massive computing power to impose structure on unstructured data that has achieved fast and widespread adoption in many fields (BIS, 2024a).

The speed of AI development and adoptions is extraordinary. Generative AI models are considered the newest technological development that can create new content. Without limitation to a defined set of potential responses in a defined format, GenAI can generate a variety of responses in various formats (Liang, 2024). They are flexible and dynamic, can learn from experience in producing responses and through ingesting new information. The escalating interest in GenAI has boosted AI adoption and we are witnessing the switch from analytical AI models created to perform specific tasks to generative AI models capable of creating human-like content (Cipollone, 2024). Simply said, GenAI enables computers to behave like humans. GenAI models reached important momentum with the launch of ChatGPT. How big of an influence it has created is best described in the numbers as ChatGPT reached 1 million users in less than a week (Aldasoro et al., 2024). ChatGPT is an AI language model developed by OpenAI that is founded on generative pre-trained transformer architecture and produced to generate human-like text based on given inputs. Although it is considered that ChatGPT may not always provide entirely accurate answers it is nevertheless significant to check or verify information produced. Recently, the newest versions of ChatGPT have been issued, including those more sophisticated. Noy and Zhang (2023) find in their research that novel versions of ChatGPT are more consistently factually accurate, while some may access the internet to fact check themselves. Thus, in more open-ended, real-world tasks, workers may consider iterative rounds of prompting and discussion with ChatGPT valuable even if they cannot instantly prompt out a final product.

According to McKinsey (2024a) survey of the adoption of GenAI, it has dramatically increased in 2023 compared to previous years, with half of the respondents saying that their organizations have adopted AI in two or more business functions, up from less than a third of respondents in 2023. Survey findings show that most organizations use GenAI in functions where its adoption could generate the most value and those are marketing and sales, product and service, as well as IT with the highest increase from 2023 recorded in marketing and sales where reported adoption has more than doubled.

In an attempt to answer the question from the introduction regarding today society's readiness for the AI era, it is very useful to take a look at the results of the AI Preparedness Index produced by the International Monetary Fund (Cazzaniga et al., 2024). The index is based on selected set of macro-structural indicators that are pertinent for AI implementation and fall into four categories: digital infrastructure, innovation and economic integration, human capital and labour market policies, and regulation and ethics. According to the findings of Cazzaniga et al. (2024) advanced economies have a larger share of high-exposure occupations compared to emerging economies and low-income countries. Accordingly, the potential to take advantages of AI will vary due to countries' preparedness and the ability of workers to adjust to new technology. Therefore, advanced and more developed emerging economies should invest in innovations and adopt adequate regulations while low-income countries and less prepared emerging economies should focus on building skilled human capital and digital infrastructure.

3. Opportunities and risks of AI

AI is transforming the ways people live and work. It is unique due to the speed with which it is spreading throughout society and the potential it has to affect economies, not to mention redefining the meaning of being human so the world needs to come together on a set of public policies to ensure AI is used for the good of humanity (Gopinath, 2023). In order to take advantages of AI, it is crucial to put humans in the centre of AI. It should support people in performing various activities, boost work efficiency, raise productivity through automation of work processes, provide higher income, and increase financial inclusion. The emergence and widespread use of AI affect the financial system stability as well as macroeconomic performance by changes in aggregate supply (through productivity) and demand (through investment, consumption and wages) (BIS, 2024a).

It is necessary to understand the way AI tools are functioning and recognize benefits and risks that they bring. Risks of AI have to be identified in order to pre-

vent incident and potential crisis situations. AI risks are difficult to forecast due to its extraordinary growth and extensive application throughout various sectors, including financial industry. Developments in AI industry such as factory robots, smart home devices, and self-driving cars are exciting as they promise higher productivity and standards of living but they can also be frightening if the machines take over (Berg, Papageorgiou, and Vaziri, 2023). As one of its utmost users, AI impacts financial systems significantly. Financial systems have used the various forms of AI since its emergence and that is constantly developing. Therefore, it is important to have clear and robust regulatory framework, as well as strong and persistent institutions to monitor and control the development of AI and its implementation in economy and financial systems. There is too much uncertainty regarding the potential extent of using AI and the power of its tools.

Numerous standards and best practices exist to help organizations alleviate the risks of traditional software or information-based systems, but the risks posed by AI systems are considered unique in many ways, making AI exceptionally challenging technology for organizations and within society as AI systems can be trained on data that can change over time, often significantly and unpredictably, thus influencing system functionality and trustworthiness in ways that are difficult to comprehend (NIST, 2023). Both AI risks and benefits can arise from the interaction of technical aspects combined with societal features related to how a system is used, its relations with other AI systems, who operates it, as well as a social context in which it is designed. Therefore, appropriate controls of AI systems are crucial so they can ease and manage inequitable outcomes. Otherwise, they can intensify, perpetuate, or exacerbate unfair or undesirable outcomes for both individuals and communities. *ISO/IEC 42001:2023, Information technology – Artificial intelligence – Management system* recommends organizations to determine the risks and opportunities according to the domain and application context of an AI system, the intended use, and the external and internal context.

Hence, development and adoption of regulation which will protect data, humanity and at the same time promote innovation is necessary. Recently, the EU adopted the Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence[1]. This regulation is supposed to be applied in accordance with the values of the Union as enshrined in the Charter of Fundamental Rights of the European Union, ensuring the protection of natural persons, undertakings, democracy, the

[1] Regulation (EU) 2024/1689 of The European Parliament and of The Council of 13 June 2024 Laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

rule of law and environmental protection, while supporting innovation and employment, thereby making the Union a leader in the acceptance of trustworthy AI. Accordingly, this regulation guarantees the free movement, cross-border, of AI-based goods and services, therefore preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by the regulation. AI is recognized in the regulation as a fast-developing family of technologies that contributes to numerous economic, environmental and societal benefits in many industries and social activities. Accordingly, AI can offer important competitive advantages in healthcare, agriculture, food safety, education and training, media, sports, culture, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, environmental monitoring, the preservation of biodiversity and ecosystems as well as climate change mitigation and adaptation. Apart from explaining numerous advantages, the Regulation (EU) 2024/1689 emphasizes that depending on the circumstances regarding AI's application, use, and level of technological development, it may produce risks and damage to public interests and fundamental rights that are protected by, in this case, Union law, including material or immaterial harm such as physical, psychological, societal or economic harm. Also, it is specified that due to potential impact that AI can have on society, a prerequisite is to build AI as a human-centric technology that serves people, with the ultimate aim of increasing human well-being.

Fiscal policies can contribute to levering the far-reaching consequences of AI. Pros and cons of imposing taxes on AI systems and products have been garnering significant attention worldwide. Brollo et al. (2024) have explored the topic with the argument for not taxing AI being production efficiency with a natural initial point for the analysis of AI and taxation being the principle that the tax system should not distort firms' production decisions, thus preserving production efficiency. On the other side, there are arguments in favour of taxing automation. These include mitigating wage inequality that arises from technological change, then alleviating excessive job displacement which comes at a social cost when technological change develops rapidly while labour market adaptation is slow because of labour market frictions. Interesting comment refers to the taxation of GenAI because, for example, jobs that are most influenced by automation through robots are not filled by unskilled workers but rather by middle-skilled routine jobs thus a tax on automation will increase the relative wages for these middle-skilled workers lowering inequality at the top but increase inequality at the bottom (Brollo et al., 2024). Accordingly, it can be optimal to either impose a tax or a subsidy on automation but implications may be ambiguous.

Although being elaborated later in the paper, table 1 summarizes implications of AI through selected macroeconomic and financial system channels including productivity, labour market and employee efficiency, monetary policy and inflation dynamics, financial stability, payment systems oversight and anti-money laundering and combating the financing of terrorism, data usage, statistics and research potential, and cyber security.

Table 1: Opportunities and threats stemming from AI

	Opportunities of using AI	Threats of using AI
Productivity	- Potential for global rise of productivity - Possibility for higher wages and incomes - Complementing people at performing activities - Automation provides workers perform more requiring activities - Improving the lives of people due to automation of activities - Greater the adoption of AI tools in economy greater the effects to productivity	- Substitute for humans - Favouring skilled over unskilled labour - Favouring automation rather than human-complementary technologies - Potential for upsurge of job losses in cognitive occupations as well - Worsening labour income when AI overtake jobs - Raising wealth inequality - Few firms' monopolistic position - AI algorithms can trigger forecasting errors in the downturn
Labour market and employee efficiency	- Releasing employees from doing daily repetitive tasks - Support employees to perform higher-productivity tasks - Substitute for exhausting paperwork - Boosting efficiency - Potential for wages' growth - Reskilling and upskilling of existing workforce - Employment of technologically skilled and qualified generations - Building innovation supportive culture in organisations	- More replaceable workers - Ability to affect cognitive jobs - Reduced labour demand and hiring - Extraordinary job losses - Lower wages and raising inability to pay debts - Disproportionate raise of income - Exacerbating inequality - Raise of long-term unemployed people lacking the necessary skills - Allocation of experts from academia to industry - Deepening of social tensions
Monetary policy and inflation dynamics	- Extensive macroeconomic and financial analysis to support monetary policy - Simplified forecasting using vast amount of granular data - Providing easy detailed comparison of prices of products and services - Using AI tools to understand factors that contribute to inflation dynamics - Downward pressure on prices when AI substitutes labour and boosts productivity resulting in a lower risk of labour shortages and descending pressure on unit labour cost growth - Supply effects - lowering energy price through improving network management and supporting more efficient energy consumption	- Prevalent adoption of AI could boost firms' ability to quickly adjust prices - Demand for highly skilled labour putting pressure on their wages while lowering demand for unskilled labour force, deepening inequality - AI may be a reason for changes in financial structure while rise in non-bank intermediation can influence longer-term interest rates as non-banks are more responsive to monetary policy measures - Influence on peoples' marginal propensity for consumption and access to credit which shows demand effects on monetary policy changes - Large computational power behind AI may influence global energy demand and upward price pressures

Financial stability	- Contributing to financial system analysis particularly useful to identify and enhance the understanding of risks in a large sample of observations - Supporting supervisors' analyses and assessments when lacking clear data for novel risks such as cyber risk and climate change risks - Regular risk assessment and their prioritization crucial to prevent breaches and risk materialization	- AI growing capability to make decisions independently and without human intervention, such as risk assessments and credit underwriting performed by AI - Market concentration due to the provision of technology services from few large firms building up considerable financial stability, operational and reputational risks - Reliance on same few algorithms may amplify procyclicality and market volatility by exacerbating herding, liquidity hoarding, runs and fire sales
Payment systems oversight and money laundering prevention	- Revolutionizing the way financial institutions detect and prevent financial crimes strengthening oversight - Improving monitoring of suspicious transactions - Using neural networks to identify suspicious patterns that are hard to detect with traditional methods - Boosting banks' operational efficiency and risk management capabilities - Enhancing customer service using tools such as robo-advisors - AI may contribute to reverse the decline in correspondent banking	- Cyber threats and cyber-attacks that can compromise prevention systems - Challenges in differentiating anomalous from regular transactions - ML weakening integrity and safety of the global financial system - Banks relying on siloed data and isolated systems for the suspicious transaction monitoring - Challenge to deliver scalability and reliability simultaneously while operating within budget limitations - AML/CFT requirements enforcement difficult with decentralized technologies
Data usage, statistics and research potential	- Improves research and analysis with speed, scale, and granularity of data as never seen before - Boosts the efficiency and effectiveness of statistical processes - Improve the quality of datasets - Support monetary policy through efficiently extracting information from various traditional and non-traditional data sources - Nowcasting, real-time data model to enhance the accuracy of forecasts	- Lack of transparency and explainability - Issues of bias and discrimination, - Challenge of guaranteeing data privacy and confidentiality for large volumes of data - Third-party dependency risks - Issues regarding consumer protection and fair lending practices - Allocation of people from academia to AI industry due to better income and possibility to develop ideas - Intellectual property rights concern
Cyber security	- Stronger cybersecurity preparedness - Sophisticated cyber threat detection - Processing of increasingly bigger data sets - Proactive cyber security and fraud prevention strategies - Building stronger resilience to cyberattacks with AI tools	- Amplified frequency of cyber-attacks - Augmented cyber risk - Social engineering, zero-day attacks and malware attacks for data leakage - GenAI imitating human behaviour increases probability of fraud - Quantum computers' power to break existing encryption models

Source: Authors' findings

3.1. Implications of AI for Productivity - Opportunities and Threats of AI

AI usage is considered beneficial for productivity growth but Acemoglu and Johnson (2023) argue that automation contribution to aggregate productivity growth is still not clear primarily as these technologies are still immature, while they could contribute to substantial productivity gains as costs fall and reliability improves. They further indicate that Goldman Sachs data suggests that AI adoption could increase productivity growth by 1.5 percentage points per year over a 10-year period and raise global GDP by 7 percent, which is equal to $7 trillion in additional output.

There are firm-level studies showing that AI could elevate annual labour productivity growth by 2–3 percentage points, on average, whereas some show nearly 7 percentage points. However, Gopinath (2023) explains that although it is difficult to measure aggregate result from these types of studies, they can raise hopes for reversing the decline in global productivity growth, which has been slowing for more than a decade. Consequently, productivity growth can increase wages and incomes, improving the lives of people around the world, and automation of activities can complement people in performing activities.

The effects on productivity and overall outcome will depend on whether we see a fast and broad-based adoption and diffusion of AI across all sectors of the economy or not although, up until now, the speed of dispersion across sectors and firms has little historical precedent (Cipollone, 2024). Automation of activities should boost overall productivity but also should not decrease worker's contribution to production. Acemoglu and Johnson (2023) consider that AI should complement rather than replace workers by empowering them to work more efficiently, accomplish higher-quality work or new tasks. However, they further point out that the AI research is predominantly focused on achieving human parity in various cognitive tasks where AI intelligence mimics and exceeds human capabilities. The latter stimulates automation rather than the expansion of human-complementary technologies. Accordingly, in order to create AI which complements workers' skills and expertise, the new technology has to be appropriately directed. It is important to develop policies which will put humans in the centre and provide benefits of AI. As GenAI can boost productivity it can also produce problems in the time of downturn as far as AI trained algorithms could trigger a series of forecasting errors, creating troubles in production and inventories, which may result in delays and scarcities of critical supplies across the global economy (Gopinath, 2024).

Brolo et al. (2024) argue that automation and robots have already replaced low- and middle-skill jobs that include routine tasks, decreasing average wages and intensifying job polarization while GenAI with intelligent automation has a potential to upsurge job losses in cognitive occupations as well. Subsequently, the labour income share in national income may deteriorate, worsening income and wealth inequality. Another significant source of risk refers to the monopolistic position of big market players. In regards to the latter, the most of the AI created value becomes extracted by a few companies, resulting in their dominance in the AI ecosystem which is consequently the key reason why productivity increased from AI at firm level may not translate into sustained value-added gains at the aggregate level, as market power upsurges costs (Cipollone, 2024). That situation is seen through the growth of IT which has led to concentration of productivity gains in the IT sector while the primarily benefiting countries are those with large and successful tech firms. A concrete example is unprecedented concentration of market value in the "Magnificent Seven" firms in the United States which are currently profiting from the AI boom and making bigger yearly profits than all the listed companies of France, Germany and Italy combined (Cipollone, 2024).

3.2. Labour market and employee efficiency - Opportunities and threats of AI

ChatGPT and implementation of other AI tools can release employees from doing daily tasks and focus on innovation thereby boosting efficiency and giving opportunity to perform higher-productivity tasks. The influence of automation and AI on labour markets depends on whether the technology is substitutable for or complementary to tasks performed by workers. Whether AI represents an opportunity or risk for employment depends on the net effect (Cipollone, 2024). Building culture that supports innovation is very important. That will influence employees to embrace changes more openly instead of being reluctant to it. The AI can present a great base for further investment into education and skills of employees. That involves reskilling and upskilling existent workforce as well as attracting new employees who are already skilled, technologically educated and qualified for novel job descriptions. ISO/IEC 23894:2023, *Information technology – Artificial intelligence – Guidance on risk management* recommends that organizations engaged in the design, development or deployment of AI systems should monitor the human and cultural landscape in which they are situated. Further, organizations should concentrate on recognizing how AI systems or components interact with pre-existing societal patterns that can influence equitable outcomes, privacy, freedom of expression, fairness, safety, security, employment, the environment, and human rights broadly.

Berg et al. (2023) explain the impact of technological change, automation, and robots on inequality and highlight four main channels that influence inequality: technological change that advances the productivity of skilled more than unskilled workers; reductions in the cost of capital that complement mainly skilled labour; amplified ability of machines to replace workers completely for particular tasks; and augmented concentration of market power in a few firms as a result of technology.

Though historically automation and information technology were used to influence routine tasks, the AI is different in having the ability to affect high-skilled jobs. Accordingly, there are findings that in advanced economies, about 60 percent of jobs may be impacted by AI (Georgieva, 2024). Roughly half of jobs exposed to AI may benefit from those developments boosting productivity, while for the other half, AI applications may perform main tasks currently performed by humans thereby decreasing labour demand, leading to lower wages and reduced hiring while in the most extreme scenario some of these jobs may vanish (Georgieva, 2024). The effect on labour income will mainly depend on the degree to which AI will complement high-income workers so if it significantly complements them, that may result into a disproportionate rise in their labour income (Georgieva, 2024). Furthermore, increases in productivity from firms that adopt AI will likely improve capital returns and consequently favour high earners, which will exacerbate inequality.

Gopinath (2024) warns that AI could turn usual downturn into a deep economic crisis by triggering large-scale disruptions in labour markets, financial markets, as well as supply chains. Accordingly, in an economy where AI is predominant, the future downturn will result in more replaceable workers than ever seen before, leading to extraordinary job losses and long-term unemployed because many displaced workers will lack the necessary skills. Consequently, many unemployed workers could struggle to repay their debts causing a main shock to the financial system.

This brings conclusion that AI will most likely deteriorate overall inequality, implying that policymakers should act proactively to prevent the technology from further amplifying social tensions. In regards to the latter, countries should establish comprehensive social safety nets and offer retraining programs for vulnerable workers. The extraordinary power of AI in research has started to allocate people from academia to industry due to the enormous potential of AI usage and rise of many start-ups that implement AI. Computer science professors are leaving academia and continue their research at the growing AI industry, realizing their ideas through start-ups.

3.3. AI effects on monetary policy

AI is very useful for macroeconomic and financial analysis, therefore, central banks apply them broadly to support monetary policy decisions (Araujo et al., 2024). AI tools can be very useful as they can analyze enormous amount of unstructured data. For instance, they can support consumers to compare prices. Granularity of data simplifies forecasting and analyzing of huge amounts of available data. As the AI develops at the speed never seen before, it is important to consider the emergence and the level of usage of different AI models, including those more sophisticated which can further influence inflation dynamics. There are possibilities that if demand for AI increases and consequently the need for highly skilled labour, that will put pressure on the wages while lowering demand for unskilled labour force that will in turn further deepen inequality. Cipollone (2024) explains the possibility for downward pressure on prices when the net effect of AI is that it substitutes labour and boosts productivity, which results in a lowered risk of labour shortages and descending pressure on unit labour cost growth.

AI has a potential to affect the financial system and economy, the latter through productivity, consumption, investment and labour markets, which consequently affect prices as well as financial stability, thus raising concerns for monetary regulators. Accordingly, as a reaction to macroeconomic changes, extensive adoption of AI could expand firms' ability to rapidly correct prices and thus impact inflation dynamics (BIS, 2024a). The greater the usage of AI, including in smaller firms, the more exacerbated its effects. Accordingly, increased uniformity and flexibility in pricing can lead to larger and faster pass-through of aggregate shocks to local prices, and hereafter inflation, compared to historical experiences (BIS, 2024a).

Central banks use AI tools to analyze various data to better understand factors that influence inflation dynamics. Accordingly, neural networks can process more input variables compared with traditional econometric models, which enable them to work with granular data sets rather than only with aggregated data which further can reflect complex non-linear relationships, providing useful insights during periods of rapidly changing inflation dynamics (Araujo et al., 2024). Neural networks can, for instance, break down services inflation into diverse components showing how much inflation is due to past price upsurges, inflation expectations, the output gap or international prices.

AI can influence monetary policy because it can be the reason for changes in financial structure. Therefore, a rise in non-bank intermediation can impact long-

er-term interest rates such as asset purchase as non-banks are more reactive to monetary policy measures than banks and non-banks demonstrate more credit, liquidity and duration risk compared with the banking sector (Cipollone, 2024). In regards to AI impact on labour market, income and wealth distribution, the AI can influence peoples' marginal propensity for consumption, access to credits and ability to pay debts, showing how demand reacts to monetary policy changes.

AI may stimulate energy price movements in both directions. Through supply side, it could lead to lower energy prices through improving network management and supporting more efficient energy consumption (Cipollone, 2024). Large computational power behind AI's development may influence global energy demand creating upward price pressures.

3.4. Implications of AI for financial stability

AI tools are used to identify and improve the understanding of risks using huge sample of observations. Supervisors in central banks use and analyze an extensive amounts of data sources to efficiently monitor financial institutions. The sources comprise of various text documents, including news articles, internal bank documents or supervisory assessments, with researching ever rising volume of data being time-consuming. At the same time, supervisors lack high quality data for some segments such as climate change and cyber risks assessments which have emerged among supervisory priorities. Hence, AI model can help them manage large variety of unstructured data. Accordingly, training models on supervisory content together with NLP techniques can classify public and supervisory documents, assume sentiment analyses and identify trending topics (Araujo et al., 2024).

The reliance of market participants on the same handful of algorithms could lead to financial stability risks (BIS, 2024a). These could arise from AI's ubiquitous adoption throughout the financial system and its growing capability to make decisions independently and without human intervention at a speed far beyond human capacity. The behaviour of financial institutions using the same algorithms could amplify procyclicality and market volatility by exacerbating herding, liquidity hoarding, runs and fire sales, concerns about dependence on a few external providers. Large economies of scale mean that the most powerful foundation models are provided by a small number of large technology companies while apart from general risks that market concentration poses to innovation and economic dynamism, this high concentration of resources could build

up considerable financial stability, operational and reputational risks (Araujo et al., 2024).

As far as financial services industry has adopted AI technology to numerous applications very quickly, including support to conduct risk assessments and credit underwriting and recommend investments, risks have built up including lack of transparency behind AI technology which will complicate decision analysis when things go wrong (Gopinath, 2023).

In order to prevent the risk materialization stemming from misuse of data risk prioritization is very important (NIST, 2023). However, risk prioritization differs between those AI systems that are created to directly interact with humans as compared to those AI systems that are not. Higher initial prioritization is more necessary when AI system is trained on large datasets that include sensitive or protected data or where the outputs of the AI systems have direct or indirect impact on humans (NIST, 2023). Unlike the latter, the AI systems deployed to interact only with computational systems require lower initial prioritization. However, regular assessment of risks and their prioritization is crucial to prevent breaches and risk materialization.

3.5. Payment system oversight and prevention of money laundering - opportunities and threats stemming from AI

Even though efficient and well-functioning payment systems are essential to the financial system stability, the immense volume of transaction data, frequently with a highly skewed distribution, poses challenges in differentiating anomalous from regular transactions (Araujo et al., 2024). Thus, early identification of suspicious payments is critical for preventing potential bank failures, cyberattacks or financial crimes.

Today, market requirements include digital, fast and non-stop available payments. Digital payments, also called electronic payments, include the transfer of value using digital devices or channels, and encompass bank transfers, mobile money, quick response (QR) codes and payment instruments such as credit or debit cards as well as the use of cryptocurrencies, such as bitcoin or so-called stablecoins, and central bank digital currencies - CBDCs (Aguilar, Frost, Guerra, Kamin and Tombini, 2024). Banks are under pressure from the rise of digital money providers, hence feeling obliged to respond by providing more attractive services. Payment modernization is necessary and brings a lot of benefits, including the provision of simpler, faster and cheaper payment transactions, boosting

financial inclusion, cash usage reduction, strengthening market competition, and lowering informal economy. On the other side, digital payments are exposed to attackers so it is important to carefully use digital services as they bring risks that should be diminished. Hence, payment systems oversight plays a crucial role in preventing fraudulent activities.

Money laundering is a global problem that weakens the integrity and safety of the global financial system (BIS Innovation Hub, 2023a). It is defined as the act of hiding the origin of illegal assets, often including a sequence of transactions that may give the impression of being legitimate on the surface. Accordingly, financial institutions have crucial role in detecting and preventing these activities, since they serve as the "first line of defence" but still most of them rely on siloed data and isolated systems for their suspicious transaction monitoring, thus limiting their ability to detect complex cross-border and cross-institutional money laundering networks.

Banks have been deploying artificial intelligence and machine learning (AI/ML) applications for various purposes, including back office and front office functions. So far, use cases refer to credit underwriting, trading activities, pricing models, regulatory capital and planning, liquidity requirements and planning, fraud detection and prevention, anti-money laundering and combating the financing of terrorism (AML/CFT), chatbots and marketing (BIS, 2024b). Hence, AI/ML practices can boost banks' operational efficiency and risk management capabilities, strengthen fraud detection, contribute to enhancing customer service such as robo-advisory services. In regards to that the use of advanced technologies in AML transaction monitoring has the potential to revolutionize the way financial institutions detect and prevent financial crimes whereas one of critical issues in AML efforts is balancing the need to detect suspicious activity with the need to protect privacy (BIS Innovation Hub, 2023a). Subsequently, the key measures of policymakers should refer to the adoption of a new set of regulations which will guarantee payment security and regulate all aspects of transactions, with a particular emphasis on protecting personal data (Fabris, 2019).

By using graph neural networks in the context of AML transactions monitoring and analysis, it may be possible to identify suspicious patterns and anomalies in transaction networks that can be hard to detect with traditional methods. Still, there is the other side to consider since machine learning models using network features could suffer from data bias and interpretability issues whereas data ethics and the explainability of automated decisions, as well as the role of human review, would require significant attention (BIS Innovation Hub, 2023a). Also, financial institutions, including banks, will be focused on improving fraud de-

tection, allowing virtual assistants, and creating recommenders to produce next best actions. In that process they are experiencing significant challenges as AI is complex and is difficult to deliver scalability and reliability simultaneously and needs to operate within the budget limitations of the bank (Papenbrock and Ashley, 2022). On the other side, fraudsters are using GenAI to produce fake calls to bankers to get the bank itself to steal money from clients on the fraudster's instructions. In regard to the latter, new identities will be backstopped by AI generated histories and money will be laundered using flows planned and ultimately accomplished by AI to escape detection (Papenbrock and Ashley, 2022).

In regards to financial integrity, decentralized technologies predominantly create new challenges, for example, blockchain based technologies. Hence, when transaction verification is decentralized and the number of entities that are included (for instance cryptocurrency exchanges, governance bodies, wallet providers, client fund managers, and market makers) is big and fragmented across firms, sectors, and countries, enforcement of AML/CFT requirements is hard (Tobias and Mancini-Griffoli, 2021).

Referring to payments, a key use case of AI models is improvement of know-your-customer (KYC) and AML processes through improving the ability to understand the compliance and reputational risks that clients might carry, due diligence on the counterparties of a transaction, the analysis of payment patterns, and anomaly recognition (BIS, 2024a). Accordingly, by bringing down costs and reducing risks through greater speed and automation, AI may contribute to reverse the decline in correspondent banking. Due to intensified customer verification and AML requirements, banks have systematically retreated from the correspondent banking business while such retreat fragments the global payment system, keeping some regions less connected with the rest of the financial system. The weakening in correspondent banking is part of general de-risking trend, with returns from processing transactions being minor compared to the risks of consequences from breaching AML/CFT requirements (BIS, 2024a).

3.6. Data usage, statistics and research - opportunities and risks arising from AI

Automating information extraction with AI provides the option of analysing various data at a speed, scale, and granularity levels that were neither imaginable nor feasible before. Accordingly, AI application in statistical processes can be very beneficial as it boosts efficiency and effectiveness. Machine learning can be considered as an extension of traditional statistical and econometric techniques.

As far as central banks rely broadly on macroeconomic and financial analysis to support monetary policy in the complex environment, efficiently extracting information from a wide range of traditional and non-traditional data sources is a substantial challenge (Araujo et al., 2024). Therefore, machine learning offers valuable tools.

AI can be used to improve the quality of datasets, from identifying and matching observations across datasets to exploiting modern machine learning techniques for quality guarantee and large language models (LLMs) to the ways that were not possible before (Cipollone, 2024). The latter has unlocked novel and non-traditional data sources including unstructured data sources like text, image, video or audio which can complement and improve existing data collections. As it is not based on pre-specified model or on statistical assumptions such as linearity or normality, a machine learning model is fitted to data through the process of training which refers to predicting outcomes on previously unseen data (Araujo et al., 2024).

Many central banks have been implementing nowcasting models for economic analysis. Nowcasting is a technique that applies real-time data to deliver timely insights that can considerably enhance the accuracy and timeliness of economic forecasts, especially during periods of intensified market volatility (BIS, 2024a). The goal is to create high-frequency real-time assessments and estimates such as gross domestic product growth or inflation, which can be simply updated once the new data are available. Still, this method is presently facing two main bottlenecks due to limited timely data and the need to pre-specify and train models for concrete task while LLMs and GenAI should overcome both challenges.

A very promising project that is aimed at collecting and scaling information about climate risks is Project Gaia (BIS Innovation Hub, 2024) – a collaboration between the BIS Innovation Hub Eurosystem Centre, the Bank of Spain, the Deutsche Bundesbank and the European Central Bank – which leverages potential of GenAI to facilitate the analysis of climate-related risks in the financial system. By automating information extraction, Gaia opens up the possibility of analyzing climate-related indicators at a scale that was not formerly feasible (BIS Innovation Hub, 2024). Furthermore, Gaia offers harmonised metrics despite the heterogeneity of naming conventions and definitions across different jurisdictions while the combination of semantic search together with iterative and systematic LLM prompting empowers Gaia to overcome differences in disclosure frameworks. That resulted in providing necessary transparency and comparability of climate-related information.

Application of AI has been reshaping the research. An example of how AI impacts and has reformed research is its deployment at the Harvard University where in December 2021, Mark Zuckerberg and Priscilla Chan, former students, pledged $500 million to create the Kempner Institute for the Study of Artificial and Natural Intelligence (Duffy, 2024). While changes in academia go slowly, AI research was succeeding at fast pace so while the Kempner Institute was gathering faculty and creating administrative infrastructure in 2022, ChatGPT was launched and become the fastest-growing consumer application in history with 100 million users in two months. Going back to necessary investment for AI development, even initial $500 million seemed to be a small amount for AI industry as the largest AI models cost a few million dollars to build in 2021, but by June 2024, the cost for training a frontier model might surpass $1 billion (Duffy, 2024). Consequently, due to big difference in funding, some professors have moved from academia to industry to develop their ideas.

Lack of transparency and explainability is a potential risk stemming from AI usage. According to *ISO/IEC 23894:2023*, the complexity of AI technologies brings challenges related to transparency and explainability of AI systems. The diversity of AI technologies further drives these challenges due to characteristics such as multiple types of data modalities, AI model topologies, and transparency and reporting mechanisms that should be selected per stakeholders' needs. Stakeholders can support setting the goals and describe the means for enhancing transparency and explainability of AI systems.

The convenience of digital services brings various risks. Issues of bias and discrimination and data privacy are significant to counter in regard to AI application. The first refers to consumer protection and fair lending practices (BIS, 2024a). The second relates to the challenge of guaranteeing data privacy and confidentiality when dealing with growing volumes of data. As far as financial institutions are obliged to comply with strict privacy standards and regulations, this can amplify legal risks. In dealing with risks stemming from AI, organizations may face tough decisions in certain scenarios in balancing, for example, between optimizing for interpretability and achieving privacy or they may experience tradeoff between predictive accuracy and interpretability (NIST, 2023). Accordingly, under some specific conditions such as data scarcity, privacy-enhancing techniques can cause loss in accuracy, thereby influencing decisions.

In order to protect data, the adoption of appropriate regulation is necessary as many AI applications process personal data. According to the European Parliamentary Research Service Study "The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence" (EPRS, 2020), AI is not explicitly

mentioned in the GDPR, but numerous provisions in the GDPR are pertinent to AI, and thus many are challenged due to the novel ways of processing personal data empowered by AI. The latter certainly produces a tension between, on the one side, the traditional data protection principles which include purpose limitation, data minimisation, the special treatment of sensitive data, the limitation on automated decisions and the full deployment of the power of AI and big data on the other side.

Third-party dependency risks arise from relying on just a few providers of AI models, which increases third-party dependency risks (BIS, 2024a). Market concentration arises from the centrality of data and the vast costs of developing and implementing data-hungry models. Heavy up-front investment is required to build data storage facilities, hire and train staff, gather and clean data and develop or refine algorithms. However, when the infrastructure is built, the cost of adding any extra unit of data is negligible.

Brynjolfsson and Unger (2023) argue that a concern can arise regarding intellectual property right as far as intellectual property law may ultimately respond and effectively prevent models from being trained on data for which the developers do not have rights. Consequently, motivations of creative professionals to produce more novel content that empowers machine learning may weaken while early AI developers may urge regulators to protect their rights. Hereafter, due to many concerns, national regulators may impose stringent regulations that slow AI development and distribution while the strictest regulation would be that some countries, businesses, and other organizations totally prohibit AI.

3.7. Cyber security - opportunities and risks stemming from AI

The introduction of GenAI models has brought both opportunities and challenges in regards to cyber security. It is perceived that AI offers more benefits than risks, especially for specific segment of cyber security such as cyber threat detection (Aldasoro et al., 2024). Application of AI systems will enable a shift from a reactive to a proactive approach to predict and neutralize threats. Still, an important issue refers to assessing the extent of autonomy to be approved to AI tools in cyber security and the nature of their interaction with humans (Aldasoro et al., 2024). Investment in human capital is crucial whilst data scientists, AI security analysts and AI supervisors are recognized as key occupations for full integration of GenAI with existing security tools.

AI models can reinforce cyber security by allowing the processing of increasingly bigger data sets with more sophisticated analytics. Application of AI methods allows users to implement more proactive cyber security and fraud prevention strategies. The interrelated world is ever more exposed to cybersecurity failures and cybercrime thus due to the widespread dependency on more complex digital systems, cyber threats are outperforming the current potential to successfully prevent and manage them (Vučinić and Luburić, 2022). As GenAI tools become more sophisticated, the frequency and speed of cyberattacks are increasing and they become more complex, owing to more developed algorithms (Aldasoro et al., 2024). Threats refer to AI-generated social engineering, zero-day attacks and malware attacks for data leakage. Accordingly, cyberattacks themselves are becoming more prevalent, sophisticated and destructive. Cyber threats are continually evolving, and are expected to become progressively disruptive as technology advances and financial systems become more interconnected. Cyber security preparedness has become increasingly significant for banks and they must act to identify vulnerabilities in their systems and remedy those weaknesses before attacks occur (Barr, 2024). However, focusing on cyber defence is not enough so the focus should be on building resilience to successful cyber-attacks, including developing and regularly testing business continuity plans. According to Risk.net (2024), firms have started to adopt their risk management practices as further advances in more sophisticated generative AI are putting pressures and may change risks.

The latest Risk.net (2024) analysis indicates that the rise in AI usage has made cyber risk the top priority risk. AI surged cyber risk to the record high level and building cyber resilience has become the priority to prevent and mitigate materialization of the cyber risk. The survey performed by Risk.net shows that many respondents expressed fear from usage of artificial intelligence in the context of cyberattacks. That consequently pushed information security to the top spot among risks whereas out of 80 major banks and financial services firms involved in the survey, 22 cited cyber-led information security risk as the top worry and 16 as the second top. Emergence of AI and building of cyber risk has put the industry's annual cyber security spending at $300 billion.

The risk of extreme losses triggered by cyber incidents has been growing while cyberattacks have nearly doubled since before the COVID-19 pandemic (IMF, 2024). Estimating a generalized extreme value distribution, the IMF results show that while most direct reported losses from cyberattacks are minor, being around $0.5 million, once every 10 years extreme cyber incident is expected to result in a $2.5 billion loss, about 800 percent of the average firm's operating income, possibly jeopardizing the liquidity and solvency of the affected firm. In the case of

financial firms, the projected maximum losses in a year are similar, around $152 million in a median year and up to $2.2 billion once every 10 years.

Recently, on July 18, 2024, the world has experienced the major cyber incident so far caused by CrowdStrike faulty Falcon content update for Windows (CrowdStrike, 2024). According to the Microsoft (2024) statement, although software updates may sometimes create disturbances, substantial incidents like the CrowdStrike event are infrequent and the estimation is that CrowdStrike's update affected 8.5 million Windows devices or less than one percent of all Windows machines. What has amplified the significance is the fact that although the percentage of affected devices was small, the broad economic and societal influences reflect the use of CrowdStrike by enterprises that run many critical services. This incident has caused disruptions across major international companies including healthcare systems, banks and air industry, resulting in thousands of delayed flights worldwide. It has also revealed the interconnectedness of the broad ecosystem consisting of global cloud providers, software platforms, security vendors and other software vendors, and customers, thereby drawing attention of everybody in the tech ecosystem to the importance of prioritizing operating with safe distribution and disaster recovery using the mechanisms that exist (Microsoft, 2024).

Quantum computers hold a potential to breach existing protection systems. So far, their usage has not been widespread but it is only a matter of time. Experts consider up to ten years, which is very fast. Quantum computers are extremely powerful, and they will probably render the existing encryption systems outdated and inadequate. Though greater usage momentum of quantum computers is uncertain, it is better to be prepared because, in the future, these computers will be very useful technological development but on the other side may pose threats to financial systems so this gives rise to the need for quantum-proofing the financial system.

4. Financial technology in the light of AI and challenges to central banks

Widespread adoption of information technology has been the key development in finance globally in recent years. Financial industry has seen a great potential in digital transformation and is the greatest user of digital technologies. Consequently, the financial sector is mostly exposed to cyberattacks so their occurrence and potential for further breaches are huge. This digital disruption brings the possibilities to increase efficiency with innovation, greater supply diversity, and

a more competitive financial system that produces market extension enhancing financial inclusion (Vives, 2019). Central banks are directly affected by AI, both as guardians of monetary and financial stability and as AI tools' users, therefore, they need to identify potential impact of AI across the economy and their own operations in order to address evolving challenges (BIS, 2024a). Without appropriate oversight, AI tools could upsurge risks to the financial system and influence financial stability (Gopinath, 2023).

When the COVID-19 pandemic occurred, some small developing countries in Africa were able to send e-money directly to people using mobile phones, while some very big and advanced countries experienced problems to put millions of cheques in the mail (Carstens, 2024). Although the picture seems incomplete, and sometimes the influence is more complicated to evaluate, in many countries, even developed ones, many people are still unbanked while even in the most technologically advanced societies, many financial transactions still take days to complete and rely on time-consuming clearing and settlement systems, particularly across national borders, while many technological solutions in the financial system still continue to occur in silos.

As Fabris and Ješić (2023) argue that the traditional standpoint is that gold represents a safe haven in periods of economic and political crisis, as well as during episodes of elevated inflation, the role it took on in the 1970s, in recent years, there has been an increasing number of studies that challenge this traditional viewpoint and doubt it. The reason for that is that in the aftermath of the Global financial crisis, cryptocurrencies have appeared with the idea of being money independent of governments and their economic policies and although cryptocurrencies do not have the basic functions of money and are more speculative, many investors have turned to them as a safe haven.

Although there is no unique definition, digital assets refer to digital representation of value or contractual rights that can be used for payment or investment purposes (FSB, 2023). They generally involve: cryptocurrencies, stablecoins, security tokens, non-fungible tokens (NFTs), and central bank digital currencies (CBDCs). Cryptocurrencies are unbacked crypto assets. Unlike them, stablecoins are defined as crypto-assets intended to maintain a stable value relative to specified asset, or a pool or basket of assets (FSB, 2023). Security tokens are digital assets that refer to security or financial investment, like stocks and bonds (PWC, 2024). NFTs include tokens that denote ownership of a unique digital item while the holder may sell, trade or redeem it.

Per definition, CBDC is defined as a digital money form denominated in the national unit of account, and is a direct liability of the central bank (Di Iorio, Kosse and Mattei, 2024). CBDC can be retail, intended for use by households and firms for everyday transactions, and wholesale, that is meant for use in transactions between banks, central banks and other financial institutions, having a similar role as today's reserves or settlement balances held at central banks.

Speaking about forward-looking technologies, it is important to consider the developments regarding quantum technology (QT). We have mentioned quantum computers in the previous section in the context of cyber risk, but they also have a strong positive potential for various industries, including financial. According to McKinsey`s (2024b) analysis, four sectors encompassing chemicals, life sciences, finance, and mobility will most likely experience the earliest effects from quantum computing and could gain up to $2 trillion by 2035. However, generating value from quantum computing is still a challenge because of limited access to state-of-the-art hardware and infrastructure, limited awareness and implementation of quantum technologies. Accordingly, the cooperation between industry, academia, and government is crucial for accelerating development of quantum technology to industrialize technology, manage intellectual property, and overcome talent gaps. In 2023, private investment in quantum technology decreased 27% year-over-year, while public investment surged more than 50%, with an emphasis on scaling established start-ups. The global public investment in quantum technology reached $42 billion in 2023, and while China and the United States had previously dominated QT public investment, other countries, particularly Germany, the United Kingdom and South Korea, made significant increases to their funding levels in quantum technology in 2023 (McKinsey, 2024b).

4.1. Embracing change and harnessing potential of AI - challenge for central banks

Regulators should be open to changes and ready to accept innovation. Still, this is not necessarily the case and regulators might be reluctant to innovations and changes because they bring new risks and often increase uncertainty. This is additional burden for central banks and regulators in financial systems because fintech is not covered by robust and strict regulatory framework unlike traditional banks. That provides the space for fintech to develop faster while banks have to comply with vigorous requirements. Challenged by fast changes in customer needs, banks invest in innovations and provide digital services, but at the same time, we have these big technology companies called Bigtechs or other fintech providers that are out of the zone of strict regulations and which take advantage

of that. To avoid that, it is important to put under control all providers of financial services and thus ensure fair market competition. Traditional banking system infrastructures cannot respond to the digital services market requirements so banks are working on innovative business models to catch up with new evolving trends. If they fail to do so, they risk fintech providers` taking over their clients, which can further jeopardize stability of individual banks and possibly pose threats to stability of the entire financial system. When assessing potential risks and developing regulatory frameworks, international organizations and national bodies consider fintech with the aim to safeguard financial stability and understand how it could be affected by fintech activities (Vučinić, 2020).

Today, the key goal of central banks refers to balancing the three strategic goals: price stability, financial stability and real economic growth (Fabris, 2024). Central banks should use AI tools in pursuit of their policy objectives and in addressing evolving challenges (BIS, 2024a). To do so, they need to upgrade their capabilities in terms of observing the effects of technological improvements also as users of the technology. As observers, they should understand AI impact on economic activity through its repercussions on aggregate supply and demand, whereas as users they have to be able to integrate AI and non-traditional data in their own analytical tools. AI will impact central banks' core activities around mandates to safeguard price and financial stability. AI will influence financial systems as well as productivity, consumption, investment and labour markets, which themselves may produce direct effects on price and financial stability. The use of AI will directly influence operations of central banks through its impact on the financial system. Financial institutions such as commercial banks progressively employ AI tools that will further transform the ways they are supervised by central banks (BIS, 2024a).

Bowman (2024) proposes principles that could help regulators become more comfortable to innovation in the banking system. The first principle refers to "understanding" innovation, its dynamics, potential impact on financial sectors, from small banks to wholesale financial markets, as well as end users. As the second principle, Bowman distinguishes regulatory openness of regulators to proposed innovation in the banking system which often, instead of openness and acceptance, rather face suspicion and concern because implementing new technology may require a change in policy or supervisory approach. The third principle involves innovation as a priority in banking and a change from a reactive approach to innovation, to the active one that promotes and facilitates innovation through transparency and open communication.

GenAI and Large Language Model systems will definitely be used for building more convenient applications such as digital assistants and intelligent chatbots, but the crucial ability is to consume a wide variety of unstructured data and then to synthesize answers to natural language queries (Papenbrock and Ashley, 2022). Tentatively, every employee and staff member can become a researcher, knowledge worker or coder. Companies, organizations, and institutions will build AI factories for intelligence production, leveraging GenAI/LLM frameworks to train, customize, validate and deploy such models. Accordingly, Papenbrock and Ashley (2022) list some examples how central banks and financial supervisors can leverage those technologies and models, including building digital assistants involving powering, enterprise search, summarization, translation, and report generation. Those are: forecasting inflation and analyzing sentiment; document management including summarizing and report creation which will optimize work for this; research and observation activities of financial systems, markets and institutions using large volumes of unstructured data like text; providing better search and responses to questions using information from multiple sources, and summarizing results; improving accuracy and generating reports regarding transaction frauds, reducing investigations and compliance risk; analysing sustainability and climate risk of the financial system as well as activities of central banks for greening the financial system; briefing news feeds and market sentiment; and understanding the impact of the central banks' own activities, programs, projects and policies.

Central banks can do a lot by encouraging innovators and fintech ideas and support the latter`s transformation into sustainable solutions. Communication between central banks and fintech innovators is important so they can better understand how to build sustainable financial models and understand regulations. Therefore, central banks have to promote responsible innovations and support sustainable financial models. This will also contribute to financial inclusion by providing digital services to those who prefer them and supporting those who, for instance, have difficulties accessing bank branches.

International cooperation is crucial. AI operates across borders and the society needs a synchronized global framework to maximize opportunities of AI while minimizing the damage to society which entails sound and smart policies that balance innovation and regulation (Gopinath, 2023). Artificial intelligence and machine learning methods can offer the opportunities to improve monitoring of AML suspicious transaction by detecting patterns and anomalies in transaction data that cannot be identified using traditional methods.

4.2. Building future-proof central banks through digital transformation

To ensure access to central bank money and preserve financial stability in this time of digital transformation, central banks are making strong efforts to respond to market requirements. They are building technological infrastructures to prevent cyber-attacks, modernizing payment systems and testing central bank currencies.

Central banks should develop clear digital strategies and transformation plans. Stakeholder engagement is crucial in that process. Central banks need innovative approaches to get the most from digital transformation. In order for an organization to be sustainably successful and to effectively and efficiently able to prevent a crisis, it has to continually review, improve and innovate its processes, products and services (Luburić, 2018).

The most recognizable means of payment is cash, as the central bank form of money. However, unlike cash, CBDC would most probably not be anonymous, but still it could guard users' data from third parties and is considered perfectly stable as a store of value compared to another digital asset (Tobias and Mancini-Griffoli, 2021). Traditional forms of money have been challenged and many people prefer paying digitally instead of in cash. Central banks want to make sure people keep trust in their currencies and ensure the access to it. Therefore, they are getting ready for digitalized world by preparing infrastructure and testing and exploring models of CBDC. In order to modernize their systems and keep pace with the latest trends, there are many examples of testing a possible central bank digital currency, which in the midst of huge exposure to the cyber environment elevates additional concerns to central banks, which strive to provide secure monetary and financial systems (Vučinić and Luburić, 2023). Soderberg et al. (2023) point out that many policy objectives of examining CBDC refer to preventing or mitigating potential future risks or guaranteeing that key central bank functions can be performed successfully in a digital future and that is popularly called future-proofing. While exploring high quality design choices, a central bank is supposed to make decisions concerning the practical experience and use of CBDC which are typically intended to a particular policy objective or reducing a particular risk. Accordingly, there can be posed account and transaction limits such as capped holdings of CBDC aimed at lowering risks of bank disintermediation. To boost flexibility there could be CBDC wallets with different caps that could also be combined with greater or lesser requirements for identification. Further it is highlighted that jurisdictions could also consider whether to limit CBDC holdings by foreigners, who can own and pay with CBDC when visiting the jurisdiction (Soderberg, 2023). Also, as technology evolves and CBDC forma-

tion as well, CBDC systems could use new technologies, whereas some of which are still unproven and could introduce new security and operational risks (BIS Innovation Hub, 2023b).

In the case of widespread adoption of CBDC, the consumers may decide to keep most of their savings in digital cash, and only allocate part of the funds to current accounts, this could pose a threat and cause a shock to the banking system triggered by the withdrawal of deposits from private banks, especially at the initial moment, and their conversion into digital cash (Kaczmarek, 2022). That may disturb the liquidity of many commercial banks, causing them to become illiquid. Therefore, the possible introduction of the above-mentioned money may result in further consolidation of the banking sector and changes in the business model of many banks, which will have to compete more effectively with cash, which will now be conveniently transferable online. According to BIS survey, 94% of 86 surveyed central banks are exploring CBDC, proceeding at their own speed, taking diverse approaches and considering different designs (Di Iorio et al., 2024). Those findings show that it is more likely that central banks will issue a wholesale CBDC within the next six years instead of the likelihood to issue a retail CBDC within the same period.

The European Central Bank (ECB) is working on the digital euro that is considered its most challenging project. A digital euro will allow usage of central bank money in digital form, that would complement cash and not replace it (Lagarde and Panetta, 2022). Accordingly, a digital euro would ensure that citizens can keep trust in the monetary anchor behind their digital payments. Lagarde and Panetta also emphasize the reasons for that, including the necessity to provide easy access to central bank money as the foundation of the currency; due to less cash in use, public money could ultimately lose its role as the monetary anchor in Europe and people's trust that private money can always be converted into central bank money could be endangered, finally damaging trust in the euro itself; then, there is also the possibility of undermining the international role of the euro, particularly if other big economies introduce CBDC that could be used for cross-border transactions.

Central banks and other regulators on the financial market have to constantly review current and explore new possibilities in order to respond to the market requirements on one side, and on the other side to make sure they are a step ahead of those who can endanger the financial system. Carstens (2024) argues that today, financial systems need timely developments in the quality and efficiency of financial services that come at relatively little cost, taking the so-called small steps approach, but they may also take big giant leaps that bring a fundamen-

tal reconsideration of the financial system and foster the development of totally new architectures. An example of the latter is tokenisation, a technology having a transformative potential for the financial system. Tokenised digital assets hold the information needed to uniquely identify assets and their owners as well as the rules and logic leading their use, thus, when properly used, tokens could increase the speed, reduce the cost and enhance the efficiency of financial transactions (Carstens, 2024).

The financial sector is consistently ranked as one of the most attacked industries, while central banks seem to be a natural target for cyberattacks, as they are accountable for the management and oversight of critical infrastructures in the financial sector such as payment system, and also keep confidential information about future policy decisions (Aldasoro et al., 2024). As AI develops, a frequency of cyberattacks increases continually. Financial sector is highly exposed to cyber risks, hence, almost one-fifth of all incidents has affected financial firms. Extreme cyber incidents in the major financial institutions hold potentials to endanger macrofinancial stability through a loss of confidence, the disruption of critical services, and due to technological and financial interconnectedness (IMF, 2024).

Besides being under constant threat from cyber attackers, central banks see opportunities in using AI primarily for the purpose of developing cyber security mechanisms, early warning systems and fraud prevention. A significant challenge for central banks is establishing the necessary IT infrastructure (Doerr et al., 2021). However, here arises another important issue and that is skilled workforce that have to be trained to use and monitor AI models and cope with innovations brought about by new generations of technology whilst the labour supply is scarce and hiring is expensive. Aldasoro et al. (2024) suggests the need for additional measures to account for the potential benefits and challenges arising from GenAI given the significant uncertainty and variability in cost estimates for potential cyber security incidents as well as benefits of establishing common guidelines and practices for all central banks.

Quick rise in the digital environment and in the interconnectedness between parties and devices relying on the internet and telecommunications networks for various purposes has formed a diverse and multifaceted cyber threat landscape which grows quickly (BIS Innovation Hub, 2023b). The volume of connected cyber-physical devices, encompassing the Internet of Things and consumer devices (such as smartphones, smart TVs, etc) is expected to be around 29.4 billion by 2030, creating a space for a huge attack. Amplified interconnectivity and data sharing between banks and third parties builds up possible challenges for data security and protection, which can be a source of additional vulnerabilities

as various parties access a bank's data. This can upsurge the likelihood of data breaches and result in a cyberattack (BIS, 2024b).

In the future, the emergence of quantum computing and its potential capacity to rapidly break encryption algorithms used in financial systems could also amplify losses from cyberattacks (IMF, 2024). Therefore, developments of quantum computers may additionally put pressure on financial system security as quantum computers can breach common encryption methods at a disturbing speed, while encryption tools that are currently used for protection can be rendered ineffective.

5. Concluding remarks

Digital transformation has significantly challenged central banks in performing their work of safeguarding monetary and financial stability as well as contributing to economic growth. As the technology develops, it is more likely that central banks and other authorities will increase the use of AI in pursuing their missions in monetary policy, financial stability and supervision. Financial systems are recognized among the most significant users of AI tools and their usage expands rapidly, so central banks are supposed to adopt their processes especially in regards to supervision activities, preventing frauds and money laundering. Artificial intelligence and machine learning methods can offer the possibility to improve monitoring of AML suspicious transaction by detecting patterns and glitches in transactions that can be overlooked by traditional methods. Although AI developments may simplify identification of risks and frauds, they can be deployed for the purpose of malicious activities as well. Evolving technologies and rapidly growing innovation in financial services could amplify cyber risks. The number of incidents caused by cyberattacks has been increasing exponentially while the possibility of using AI for that purpose has pushed cyber risk as the top concern for many organizations worldwide, with special emphasis on the financial sector as it has been recognized as being most exposed industry to cyber breaches.

It is important that as AI expands and automation accelerates so that it does not erode the job market and deepen unemployment. There are concerns coming from respective addresses from international organization that warn about a potential of AI to disrupt job markets and increase social tensions. This could be prevented thorough reskilling and upskilling existing workforce and the employment of new qualified labour. AI should complement human resources and not substitute people by taking over their jobs. Automation should be used to

increase efficiency and release workers from doing daily repetitive work and not to be a replacement for humans.

Although AI has a potential to change financial markets through introduction of new business models, investment opportunities, and efficient transaction mechanisms, its fast growth also brings about an exceptional set of challenges and risks such as fraud, data privacy issues, market manipulation, cybersecurity threats, and regulatory uncertainties.

Key takeaways:

- AI has a strong transformative potential but it can also be disruptive;
- AI tools for macroeconomic and financial analysis can support monetary policy, supervision, payment systems oversight and financial stability using huge amount of unstructured data;
- AI provides speed, scale and granularity of data unfeasible before;
- The emergence of GenAI is particularly significant because of its ability to imitate human behaviour;
- The world needs human-centric AI tools to complement instead of replace people and to boost efficiency;
- AI can deteriorate overall inequality, therefore, policymakers must proactively act to develop policies that will ensure AI is used for the good of humanity and provide benefits;
- Importance of building strong and resistant institutions with developed systems for prevention of ever raising cyber threats;
- Identification and minimization of risks stemming from AI is vital.

Central banks should encourage new fintech ideas, promote responsible innovations and support sustainable financial models. They can help transformation of innovative ideas and new approaches into sustainable solutions.

References:

1. Acemoğlu, D. and Johnson, S. (2023). Rebalancing AI. *Finance and Development Magazine*. IMF. Retrieved from: https://www.imf.org/en/Publications/fandd/issues/2023/12/Rebalancing-AI-Acemoglu-Johnson
2. Aguilar, A., Frost, J., Guerra, R., Kamin, S. and Tombini, A. (2024). Digital payments, informality and economic growth. *BIS Working Papers* No 1196. Retrieved from: https://www.bis.org/publ/work1196.pdf
3. Aldasoro, I., Doerr, S., Gambacorta, L., Notra, S., Oliviero, T. and Whyte, D. (2024). Generative Artificial Intelligence and Cyber Security in Central Banking. *BIS Paper*. No 145. Retrieved from: https://www.bis.org/publ/bppdf/bispap145.pdf
4. Araujo, D., Doerr, S., Gambacorta, L. and Tissot, B. (2024). Artificial intelligence in central banking. *BIS Bulletin* No 84. Retrieved from: https://www.bis.org/publ/bisbull84.pdf
5. Barr, M.S. (2024, January 7). Opening Remarks at Conference on Measuring Cyber Risk in the Financial Services Sector, Boston, Massachusetts. Retrieved from: https://www.federalreserve.gov/newsevents/speech/files/barr20240117a.pdf
6. Berg, A., Papageorgiou, C. and Vaziri, M. (2023). Technology's Bifurcated Bite. *Finance & Development Magazine*, IMF. Retrieved from: https://www.imf.org/en/Publications/fandd/issues/2023/12/Technology-bifurcated-bite-Berg-Papageorgiou-Vaziri
7. BIS (2024a). BIS Annual Economic Report 2024. Artificial intelligence and the economy: implications for central banks. BIS. Retrieved from: https://www.bis.org/publ/arpdf/ar2024e3.pdf
8. BIS (2024b). Digitalisation of finance. Retrieved from: https://www.bis.org/bcbs/publ/d575.pdf
9. BIS Innovation Hub (2023a). *Project Aurora: The power of data, technology and collaboration to combat money laundering*. BIS. Retrieved from: https://www.bis.org/publ/othp66.pdf
10. BIS Innovation Hub (2023b). *Project Polaris, Part 2: A security and resilience framework for CBDC systems*. BIS. Retrieved from: https://www.bis.org/publ/othp70.pdf
11. BIS Innovation Hub (2024). Project Gaia Enabling climate risk analysis using generative AI. BIS. Retrieved from: https://www.bis.org/publ/othp84.pdf
12. Bowman, M. W. (2024, May 15). Innovation and the evolving financial landscape. Speech at the Digital Chamber DC Blockchain Summit 2024, Washington DC. Retrieved from: https://www.bis.org/review/r240517a.pdf

13. Brollo, F., Dabla-Norris, E., De Mooij, R., Garcia-Macia, D., Hanappi, T., Liu, L., Nguyen, & Anh D. M. (2024). Broadening the Gains from Generative AI: The Role of Fiscal Policies. IMF Staff Discussion Note SDN2024/002, Retrieved from: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2024/06/11/Broadening-the-Gains-from-Generative-AI-The-Role-of-Fiscal-Policies-549639?cid=ca-com-homepage
14. Brynjolfsson, E. and Unger, G. (2023). The Macroeconomics of Artificial Intelligence. *Finance & Development Magazine*. Retrieved from: https://www.imf.org/en/Publications/fandd/issues/2023/12/Macroeconomics-of-artificial-intelligence-Brynjolfsson-Unger
15. Carstens A. (2024, May 6). Technological innovation: small steps and giant leaps. Speech at the https://www.thecrimson.com/article/2024/6/4/ai-boom-arrives-at-harvard/. Retrieved from: https://www.bis.org/speeches/sp240506.htm
16. Cazzaniga, M., Jaumotte, F., Li, L., Melina, G., Panton, A.J., Pizzinelli, C., Rockall, E.J. & Tavares, M.M. (2024). Gen-AI: Artificial Intelligence and the Future of Work. IMF Staff Discussion Note SDN2024/001, IMF. Retrieved from: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2024/01/14/Gen-AI-Artificial-Intelligence-and-the-Future-of-Work-542379
17. Cipollone, P. (2024, July 4). Artificial intelligence: a central bank's view. Speech at the *National Conference of Statistics on official statistics at the time of artificial intelligence*. ECB. Retrieved from: https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp240704_1~e348c05894.en.html
18. Crowdstrike (July 21, 2024). Remediation and Guidance Hub: Falcon Content Update for Windows Hosts. Retrieved from: https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/
19. Di Iorio, A., Kosse, A. and Mattei, I. (2024). Embracing diversity, advancing together – results of the 2023 BIS survey on central bank digital currencies and crypto. BIS Papers no.147. Retrieved from: https://www.bis.org/publ/bppdf/bispap147.pdf
20. Doerr, S., Gambacorta, L., and Serena,J. (2021). Big data and machine learning in central banking. *BIS Working Papers* No 930. Retrieved from: https://www.bis.org/publ/work930.pdf
21. Duffy, H. (2024). "Hyped Just About Right": How the AI Boom is Reshaping Research at Harvard. *The Harvard Crimson*, Retrieved from: https://www.thecrimson.com/article/2024/6/4/ai-boom-arrives-at-harvard/
22. European Parliamentary Research Service (2020). The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

23. Fabris and Ješić (2023). Are Gold and Bitcoin a Safe Haven for European Indices? *Journal of Central Banking Theory and Practice*, 2023, 1, pp. 27-44. DOI: 10.2478/jcbtp-2023-0002. Retrieved from: https://www.cbcg.me/slike_i_fajlovi/fajlovi/journal/vol12/jcbtp-2023-0002.pdf
24. Fabris, N. (2019). Cashless Society – The Future of Money or a Utopia? *Journal of Central Banking Theory and Practice*, 2019, 1, pp. 53-66. DOI: 10.2478/jcbtp-2019-0003. Retrieved from: https://intapi.sciendo.com/pdf/10.2478/jcbtp-2019-0003
25. Fabris, N. (2024). Monetary Policy between Stability and Growth. *Journal of Central Banking Theory and Practice*, 2024, 1, pp. 27-42. DOI: 10.2478/jcbtp-2024-0002. Retrieved from: https://www.cbcg.me/slike_i_fajlovi/fajlovi/journal/vol13/jcbtp-2024-0002.pdf
26. FSB (2023). High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements. Final report. Retrieved from: https://www.fsb.org/wp-content/uploads/P170723-3.pdf
27. Georgieva, K. (2024). AI Will Transform the Global Economy. Let's Make Sure It Benefits Humanity. Retrieved from: https://www.imf.org/en/Blogs/Articles/2024/01/14/ai-will-transform-the-global-economy-lets-make-sure-it-benefits-humanity
28. Gopinath, G. (2023). Harnessing AI for Global Good. Finance & Development Magazine. Retrieved from: https://www.imf.org/en/Publications/fandd/issues/2023/12/ST-harnessing-AI-for-global-good-Gita-Gopinath
29. Gopinath, G. (2024, May 23). Crisis Amplifier? How to Prevent AI from Worsening the Next Economic Downturn. Speech at AI for Good Global Summit, Geneva, Switzerland. Retrieved from: https://www.imf.org/en/News/Articles/2024/05/30/sp053024-crisis-amplifier-how-to-prevent-ai-from-worsening-the-next-economic-downturn
30. Hawking, S. (2016, October 19). Speech at the launch of the Leverhulme Centre for the Future of Intelligence. Retrieved from: https://www.cam.ac.uk/research/news/the-best-or-worst-thing-to-happen-to-humanity-stephen-hawking-launches-centre-for-the-future-of
31. IMF (2024). April 2024 Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks, IMF, Washington. Retrieved from: https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024
32. *ISO/IEC 23053:2022, Framework for Artificial intelligence (AI), System using machine learning (ML)*, The International Organization for Standardization and The International Electrotechnical Commission, Switzerland, 2022.

33. *ISO/IEC 23894:2023, Information technology – Artificial intelligence – Guidance on risk management*, The International Organization for Standardization and The International Electrotechnical Commission, Switzerland, 2023.
34. *ISO/IEC 42001:2023, Information technology – Artificial intelligence – Management system*, The International Organization for Standardization and The International Electrotechnical Commission, Switzerland, 2023.
35. Kaczmarek, P. (2022). Central Bank Digital Currency: Scenarios of Implementation and Potential Consequences for Monetary System. *Journal of Central Banking Theory and Practice*, 2022, 3, pp. 137-154. DOI: 10.2478/jcbtp-2022-0027. Retrieved from: https://sciendo.com/article/10.2478/jcbtp-2022-0027
36. Lagarde, C. and Panetta, F. (2022). Key objectives of the digital euro. *The ECB Blog*, 13 July. Retrieved from: https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog220713~34e21c3240.en.html
37. Liang, N. (2024). Remarks on Artificial Intelligence in Finance. *Speech at the OECD – FSB Roundtable on Artificial Intelligence in Finance*, Paris, 22 May 2024. Retrieved from: https://www.fsb.org/2024/06/remarks-by-nellie-liang-on-artificial-intelligence-in-finance/
38. Luburić, R. (2018). A Model of Crisis Prevention (Based on managing change, quality management and risk management). *Journal of Central Banking Theory and Practice*, 2019, 2. pp. 33-49. DOI: 10.2478/jcbtp-2019-0012. Retrieved from: https://intapi.sciendo.com/pdf/10.2478/jcbtp-2019-0012
39. McKinsey (2024a). *The state of AI in early 2024: Gen AI adoption spikes and starts to generate value*. Retrieved from: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai#/
40. McKinsey (2024b). Steady progress in approaching the quantum advantage. Retrieved from: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage
41. Microsoft (July 20, 2024). Helping our customers through the CrowdStrike outage. Retrieved from: https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/
42. National Institute of Standards and Technology (NIST) (2023). US Artificial Intelligence Risk Management Framework. Retrieved from: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
43. Noy, S. and Zhang, W. (2023). Experimental Evidence on the Productivity Effects of Generative Artificial Intelligence. *Science*, vol 6654, 381, pp. 187–92. DOI: 10.1126/science.adh2586. Retrieved from: https://www.science.org/doi/10.1126/science.adh2586

44. Papenbrock, J. and Ashley, J. (2022). Modern Computing Platforms as Key Technology for Central Banks, Financial Supervisors, and Regulators. *IFC-Bank of Italy Workshop on "Data Science in Central Banking: Applications and tools"*. Retrieved from: https://www.bis.org/ifc/publ/ifcb59_04.pdf
45. PWC (July 20, 2024). Demystifying cryptocurrency and digital assets. Retrieved from: https://www.pwc.com/us/en/tech-effect/emerging-tech/understanding-cryptocurrency-digital-assets.html
46. Regulation (EU) 2024/1689 of the European Parliament and of the Council (13 June 2024). *Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
47. Risk.net (2024, March 27). Top 10 operational risks for 2024. Retrieved from: https://www.risk.net/risk-management/7959161/top-10-operational-risks-for-2024
48. Soderberg, G., Kiff, J., Bechara, M., Forte, S., Kao, K., Lannquist, A., Sun, T., Tourpe, H., & Yoshinaga, A. (2023). "How Should Central Banks Explore Central Bank Digital Currency?: A Dynamic Decision-Making Framework." *IMF Fintech Note 2023/008*, International Monetary Fund, Washington, DC. Retrieved from: https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/08/How-Should-Central-Banks-Explore-Central-Bank-Digital-Currency-538504
49. Tobias, A. and Mancini-Griffoli, T. (2021). The Rise of Digital Money. *Annual Review of Financial Economics*. 2021, 13, pp. 57–77. Retrieved from: https://www.annualreviews.org/content/journals/10.1146/annurev-financial-101620-063859
50. Vives, X. (2019). Digital Disruption in Banking. *The Annual Review of Financial Economics*. 2019, 11, pp. 243–272. Retrieved from: https://www.annualreviews.org/content/journals/10.1146/annurev-financial-100719-120854
51. Vučinić, M. (2020). Fintech and Financial Stability Potential Influence of FinTech on Financial Stability, Risks and Benefits. *Journal of Central Banking Theory and Practice*, 2020, 2, pp. 43-66. DOI: 10.2478/jcbtp-2020-0013. Retrieved from: https://intapi.sciendo.com/pdf/10.2478/jcbtp-2020-0013
52. Vučinić, M. and Luburić, R. (2022). Fintech, Risk-Based Thinking and Cyber Risk, *Journal of Central Banking Theory and Practice*, 2022, 2, pp. 27-53. DOI: 10.2478/jcbtp-2022-0012. Retrieved from: https://www.cbcg.me/slike_i_fajlovi/fajlovi/journal/vol11/jcbtp-2022-0012.pdf

53. Vučinić, M. and Luburić, R. (2023). Project Management in Central Banks, *Journal of Central Banking Theory and Practice*, 2023, 2, pp. 5-31. DOI: 10.2478/jcbtp-2023-0012. Retrieved from: https://www.cbcg.me/slike_i_fajlovi/fajlovi/journal/vol12/jcbtp-2023-0012.pdf