sciendo

UDK: 336.743:004
DOI: 10.2478/jcbtp-2022-0012

Journal of Central Banking Theory and Practice, 2022, 2, pp. 27-53
Received: 30 March 2021; accepted: 10 August 2021

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

Fintech, Risk-Based Thinking and Cyber Risk

Abstract: Financial technology innovations (Fintech) are changing the provision of traditional financial services. Although they bring with them various benefits and opportunities, they also have weaknesses and pose potential threats to financial systems. The paper examines the latest developments in the area of Fintech and outlines the potential benefits and associated risks. It highlights the vital role of the monetary authorities in the context of the policies and initiatives required in order to modernize the financial system, including research and the potential issuance of central bank digital currency, while simultaneously fulfilling their core objectives of preserving monetary and financial stability. The authors highlight the importance of artificial intelligence in Fintech development. They create a Fintech SWOT to support and analyse the above. It goes on further to explain the new management concept of "Risk-based thinking" as a way to approach these potential opportunities and threats of Fintech. Finally, the paper looks at cyber risk in the Fintech landscape as the latest and potentially greatest threat springing from these turbulent and uncertain times.

Keywords: Financial Technological Innovations (Fintech), Risk Management, "Risk–based thinking", Cyber risk.

JEL Classification: E58, F65, G20, O32.

1. Introduction

The world has been changing rapidly in recent decades. To cope with the increasing speed of changes, organisations and authorities, as well as the entire population have to take timely and adequate measures in order to prevent the adverse

effects of the threats and dangers that have been increasing every day. This paper examines the importance of such preventive actions and employing "Risk-based thinking". It highlights the developments in financial technology, more commonly known as Fintech, that have greatly affected the traditional monetary and financial systems, thereby creating not only real opportunities, but also producing significant threats, notably cyber risk. The paper presents a SWOT analysis to outline the various benefits and opportunities as well as the weaknesses and risks linked to Fintech. The new management concept of "Risk based thinking" is a way to approach these potential problems and successes. By employing "Risk-based thinking", it is possible not only to act early to prevent risks but also to correct or at least reduce weaknesses and to take advantage of opportunities to boost development and emphasize strengths. Cyber risk is one of the greatest risks stemming from Fintech, therefore, it is additionally analysed in the paper through the prism of financial innovations and "Risk-based thinking".

The development and implementation of digital technologies have helped reshape the economic and financial processes around the globe. The Covid-19 pandemic has further accelerated these processes and contributed to the faster adoption of digital technologies in the financial sector. People are now increasingly demanding that payments provided through digital services are fast, inclusive and convenient. While Fintech supports financial inclusion, creates new jobs, inspires innovation and simplifies access to financial services, it also exposes people, systems and authorities to new risks that could jeopardize smooth functioning of processes and existing policies. Fintech provides more efficient and convenient payment options, but also brings with it various risks in terms of competition, privacy and financial stability. Accordingly, many people are concerned about privacy issues, the trustworthiness of the systems, cybersecurity and any potential exposure to cyberattacks.

The new global technology companies, the so-called BigTechs use their market share and influence to expand their activities into the payment landscape, thereby threatening traditional financial services. These BigTechs already operate with a large volume of collected data and could interfere with other financial services such as bank lending. The development of the new crypto currencies and stablecoins provided by BigTechs could disrupt the traditional monetary and payments systems and jeopardize financial stability. In order to prevent the materialization of risks, the monetary and financial authorities are carefully examining this technology driven innovation in terms of its impact, benefits and risks. They are creating new regulatory policies adjusted to the latest financial service trends. Simultaneously, many central banks are exploring possible versions of central bank digital currency (CBDC). The monetary and financial authorities are mak-

ing great efforts to respond to market demand and consumer needs through support for innovative payment solutions. At the same time, however, they are facing significant challenges because they have to stay dedicated to achieving their core goals - preserving monetary and financial stability.

Building up a strong and resilient financial system is of the utmost importance in order to adequately respond to all potential threats and mitigate the associated risks. Cybersecurity is an extremely important topic in this effort and directed towards building financial systems resistant to cyber risks and cyberattacks. In order to survive, develop and be successful in these times of rapid changes accompanied by complex risks, it is essential to effectively and efficiently manage the risks.

The paper is organized as follows. After the introduction, the second part discusses the latest developments in Fintech, central bank digital currency, and the importance of artificial intelligence for Fintech. The authors also create a Fintech SWOT analysis to highlight the above. The third part discusses the concept of "Risk-based thinking" in terms of preventing undesirable results, while the fourth part deals with cyber risk in the Fintech landscape. The fifth part concludes the paper.

2. Fintech - Transforming Financial Processes

Fintech innovations have brought with them new habits, reshaped communication channels between financial service providers and consumers, and opened up space for the inclusion of those without bank accounts or who are not properly represented in traditional financial systems. The Financial Stability Board (FSB, n.d.) defines Fintech as "technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services". Distance working and lockdowns during the Covid-19 pandemic has significantly speeded up the use of financial digital services.

People are interested in fast, instant, and convenient payment services available through various electronic devices and mobile applications. As Panetta (2020) explains, Fintech is triggering a revolution in the financial sector, which brings about not only innovation but also risks. Therefore, despite the beneficial sides of Fintech and its contribution to financial inclusion, there are risks that go hand in hand with digital financial innovations and they require careful attention by regulators, providers and consumers. Those risks are cybersecurity and opera-

tional risks, consumer protection risks such as data protection and privacy, and prudential and macro-financial risks (Cambridge Center for Alternative Finance and World Bank Group, 2020). There are risks of outsourcing of specific activities by financial institutions, as well as, making sure to manage third-party risk properly. Even though Fintech provides financial services at reduced costs, improved efficiency, and with all the new data and computing power available, it is still prone to the same risks traditionally present in finance such as credit, liquidity, market, and operational risks which can be condensed or transferred, but not excluded completely (Feyen, Frost, Gambacorta, Natarajan and Saal, 2021). Market failures can influence financial stability, threaten security, cause spillovers, and induce systemic risks. These risks and threats are amplifying as digital financial services expand.

Digital financial innovations have influenced major improvements in the systems' connectivity and computing power that resulted in a great amount of newly created and usable data (Feyen et al., 2021). An example is the rapid expansion of BigTechs that can increase financial inclusion, lower the costs of products and services, and develop greater consumer choice in the short term (Bains, Sugimoto and Wilson, 2022). However, by utilizing their strong and diverse business models as well as the competitive advantages stemming from data analysis, network externalities, and their intertwined activities loop, they are increasing their presence and market share in financial services (Bains et al., 2022). This raises an important policy issue regarding competition in the market and concentration risks. Market players who concentrate data and amplify their influence could diminish intermediation costs and increase overall inclusion, but such a high level of concentration on the market is unfavourable. They can exacerbate the risk of the misuse of personal data for commercial or other purposes while endangering privacy and competition.

The development of blockchain based on Distributed Ledger Technology (DLT) and the creation of cryptoassets have disrupted traditional methods of payments and doing business. There are arguments in favour of DLT as having the ability to contribute to greater transparency and reduce complexity by decreasing traditional dependence on a central ledger managed by a single entity entrusted with holding and transferring funds. On the other hand, many people warn that DLT has the potential to disrupt payments and settlements and bring about increased risks (Vučinić, 2020). These risks include some very important issues such as cybersecurity and the prevention of abuse of consumers' accounts, deposits and personal data. As regards the latter, ensuring cybersecurity has already become an important matter for authorities.

Central banks manage financial risks as well as non-financial risks. Recent important developments such as climate change, overall economic trends, financial inclusion, Fintech and cybersecurity have further amplified the awareness of non-financial risks for the central bank and reinforced the need for enhanced central bank risk management (Khan and Malaika, 2021). The risks to the central bank, including those related to IT, operational risks associated with Financial Market Infrastructures (FMIs), and the setting up and maintenance of infrastructure for settlements systems have all drawn significant attention. Khan and Malaika point out that Fintech can pose policy risks associated with several key central bank functions including monetary policy, payment systems, operations and oversight, financial supervision, cash management, reserve management, financial integrity and financial inclusion.

The rapid development of Fintech calls for more oversight and supervision from regulators. Although, it is very challenging and requires a large volume of new or revised regulation, research, development, human capacities and financial resources, the global trend is obvious and authorities throughout the world have shown their openness to adapting to new global trends and responding to consumers' needs. A concrete example is the ongoing research regarding a central bank digital currency - CBDC. Central banks are examining the possibilities, diagnosing the benefits and weaknesses and are preparing appropriate systems if required, while, at the same time, they are still obliged to fulfil their primary goals of safeguarding monetary and financial stability. The primary objective of a central bank is to act preventively to preclude a crisis (Fabris, 2018) and safeguard financial stability.

Collaboration among authorities is essential as the responsibility for these changes lies with the different public institutions. This cooperation is important both at national and international levels. Regulatory authorities are constantly performing activities to manage the policy trade-offs between: stability and integrity; competition and efficiency; and consumer protection and privacy (Feyen et al., 2021). They must find a balance between innovation and efficiency. The appearance of new entrants on the financial market brings a range of potential challenges for supervision authorities in terms of policy enforcement and consumer protection. The creation of new anti-trust rules for the digital era, data mobility requirements and data protection laws may help to alleviate the risks stemming from such policy trade-offs. Stronger international cooperation is necessary in terms of cyber security, anti-money laundering and the combating of financing terrorism, the development of regulatory and supervisory frameworks, as well as payment and securities settlement systems and cross-border payments (Vučinić, 2020).

International institutions have placed the rapid technology driven developments in financial services among the priorities in their policies. The International Monetary Fund (IMF, 2018) Bali Agenda set out a list of policy elements aimed at helping member countries to harness the benefits and opportunities of the rapid developments in financial technology that are changing the provision of banking services, while also effectively managing the inherent risks. Recognizing the rapid pace of Fintech development and the major consequences that it will produce for global financial systems and central banks, the Bank for International Settlements (BIS) has established Innovation Hub Centers in Hong Kong SAR, Singapore, Switzerland, London and Stockholm. It will soon be opening centers in Toronto and for the Eurosystem in Frankfurt/Paris (BIS, 2021a). In addition, the Innovation Hub network has established a strategic partnership with the Federal Reserve System through the New York Innovation Center of the Federal Reserve Bank of New York.

Another important area of innovation refers to the new technologies that helps authorities to improve their supervisory capabilities, the so-called "SupTech' and by new institutions created to meet their regulatory requirements known as '"RegTech". Both the SupTech and RegTech tools could have significant benefits for financial stability. SupTech could improve oversight, surveillance and analytical capabilities, and generate real time indicators of risk to support forward looking, judgement based, supervision and policymaking (FSB, 2020a). SupTech and RegTech tools could contribute to enhancing cybersecurity and the prevention of financial crime while also supporting authorities in their efforts to combat money laundering, terrorist financing, bribery, corruption and insider trading (FSB, 2020a).

2.1. Developments in the field of Central Bank Digital Currency

The development of cryptocurrencies and private sector-owned stablecoins have intensified the research into the further modernization of payment system infrastructure including the introduction of central bank digital currency. The so-called stablecoins are an attempt to address the high volatility of "traditional" cryptoassets by anchoring their value to one or more other assets, such as sovereign currencies. Stablecoins have the potential to increase efficiencies in payments (including cross-border payments), and encourage greater financial inclusion (FSB, 2020b). However, in the case of a wider adoption of stablecoins in which they become a means of payment and/or a store of value in multiple jurisdictions at a substantial volume, it could lead to the creation of a global stablecoin (GSC) and influence financial stability.

According to Panetta (2020), the BigTechs may contribute to the rapid acceptance of stablecoins, both domestically and across borders. He also argues that stable coins raise concerns about consumer protection and financial stability as long as the issuer of a stablecoin cannot guarantee the certainty of the value of the payment instrument it offers as such a guarantee can only be provided by the central bank. Unlike bank deposits stablecoins do not benefit from deposit guarantee schemes, their holders cannot rely on the level of inspection that is the norm in banking supervision, and the issuers do not have access to central bank standing facilities. As the author highlights, this makes stablecoin users prone to higher credit, market and liquidity risks, and the stablecoins themselves are vulnerable to runs, with potentially systemic consequences.

While being committed to creating innovative, inclusive, competitive and resilient payment systems, monetary authorities are facing various challenges. One of them involves the potential introduction of CBDC. That is a form of digital money, denominated in the national unit of account and is a direct liability of the central bank (BIS, 2021b). CBDCs are designed as either a wholesale CBDC for use among financial intermediaries only or as retail CBDCs for use by a wider economy. On the one hand, CBDC presents opportunities including the greater effectiveness of the transmission of monetary policy, cost reduction in the production and distribution of cash, facilitating cross-border payments, further innovation and financial inclusion. On the other hand, CBDC can pose significant challenges for central banks including the risk of disintermediation, cyber risk, rapid runs on central bank money, and increases in bank funding costs while cross-border CBDC could create pressures for currency substitution. Although technological developments in money and payments could bring about various benefits, the ultimate outcome for the well-being of individuals in society depends on the market structure and governance arrangements that reinforce it (BIS, 2021b). In regards to the latter, the same technology developments that could contribute to greater access, lower costs and better competition, could also induce engrained market power and data concentration.

While this new generation of infrastructures based on DLT emerge, it is important that central banks remain up-to-date with technological advances that could possibly interfere with the smooth functioning of the financial systems. As of mid-July 2021, some 56 central banks had published retail or wholesale CBDC reports and three countries (Ecuador, Ukraine and Uruguay) had completed a retail CBDC pilot, eight other retail CBDC pilots are ongoing, including in China, Korea and Sweden (Auer et al., 2021).

To add on the latter in July 2021 the Governing Council of the European Central Bank (ECB) decided to launch the investigation phase of digital euro project aimed to address key issues regarding design and distribution (European Central Bank, 2021a). The investigation started in October 2021 and will last for two years (ECB, n.d). Digital euro would combine the efficiency of a digital payment instrument with the safety of central bank money and would complement cash and not replace it and therefore these two types of money would be available to all (Panetta, 2020).

The success of a retail CBDC would depend on a proper division of work between the central bank and the private sector. Auer and Böhme (2021) explored possible designs of retail CBDC architectures. The examples differ in terms of the structure of legal claims and the record kept by the central bank. One example is "Direct CBDC", when the CBDC is a direct claim on the central bank and it handles all payments in real time and therefore keeps a record of all retail holdings. In this case, central bank is the only institution handling payment services. Besides this single-tier, CBDC Auer and Böhme (2021) present two-tier structures with direct claims on the central bank while intermediaries handle real-time payments. Accordingly, there are possibilities that central bank either retains a copy of all retail CBDC holdings named "Hybrid CBDC" or only run a wholesale ledger so-called "Intermediated CBDC". Auer and Böhme (2021) also distinguish an alternative design called "Indirect architecture", but it is not a retail CBDC as the central bank only operates the wholesale payment system. Central bank both issues and redeems the CBDC indirectly to intermediaries while intermediaries in turn issue claims to consumers. Accordingly, the intermediary is obliged to back fully each claim with a CBDC holding at the central bank.

Which model may best suit the central bank depends on many factors. In terms of privacy and data security, some banks might be more interested in considering an "Intermediated" CBDC architecture, in which the central bank records wholesale balances only, which reduces the risk and impact of data breaches at the central bank. The main disadvantage of the latter is that the central bank needs to honour claims that it has no record of and, consequently, it has to rely on the integrity and availability of the records kept by third parties (Auer and Böhme, 2021). As the authors argue, the "Hybrid" and "Intermediated CBDC" architectures would have better financial resilience than fully backed payment accounts and they appear to be simpler to operate for the central bank than a "Direct CBDC". In regards to the latter, as the central bank does not directly cooperate with retail users, it can focus on a limited number of core responsibilities, while competing intermediaries handle the operation.

Soderberg et al. (2022) also differentiate among three conceptual CBDC models, similar to the above mentioned. When a central bank performs all functions in the payment systems, from issuing CBDC to distributing it including direct interaction with end users, the authors refer to it as "Unilateral CBDC". The second model named "Intermediated CBDC" refers to the infrastructure when a central bank issues CBDC but then delegates other functions to non-central bank intermediaries who interact with end users and this model can take different forms depending on the distribution of functions between the central bank and private intermediaries. There is also a third model, the so-called "Synthetic CBDC" (sCBDC) when private firms issue digital currency that is backed by central bank assets that they acquire from the central bank. In fact, the latter is not a CBDC, but rather a stablecoin or a special type of e-money not issued by a central bank.

An important issue that occurs in the case of two-tier CBDC architectures refers to the regulations and/or supervision of intermediaries. The trade-off between operational and supervisory complexity emerges for central banks thus, they can operate either a complex technical infrastructure or a complex supervisory regime (Auer and Böhme, 2021).

CBDCs have the potential to improve the efficiency of cross-border payments. However, there is a need for the coordination of national CBDC designs in order to contribute to more efficient cross-currency and cross-border payments. Also, there is a space for other improvements including offering secure settlement, decreasing costly and lengthy intermediation chains in the payment process, and removing operating hour mismatches by being accessible 24/7 (BIS, 2021c).

Central banks are also actively carrying out wholesale cross-border CBDC experiments. One of those projects is the Jura project. Several central banks are exploring use cases for wholesale CBDCs (wCBDC), with a view to potentially supporting a safe financial ecosystem. Project Jura explored the direct transfer of Euro and Swiss Franc wCBDC between French and Swiss commercial banks on a single DLT platform operated by a third party (Bank of France-BdF, Bank for International Settlements-BIS and Swiss National Bank-SNB, 2021). The test operated in a near-real setting, with real-value transactions and met all the current regulatory requirements. The issuance of wCBDC on a third-party platform and giving non-resident financial institutions direct access to central bank money raises a number of complex policy issues. Project Jura explores a new approach involving subnetworks and dual-notary signing, which may give central banks the confidence to issue wCBDC on a third-party platform and to provide non-resident financial institutions with access to wCBDC (BdF, BIS, and SNB, 2021).

2.2. The Importance of Artificial Intelligence for Fintech Development

Advances in artificial intelligence (AI) are very important for Fintech developments. It offers not only new opportunities but also new challenges to the financial systems. AI systems accomplish complex, problem-solving tasks in a way that is similar to how humans would resolve problems (Malone, Rus, and Laubacher, 2020). Machine learning (ML) is a subfield of AI that refers to a process which begins with a body of data and then tries to derive rules or procedures to use that data or envisage potential future data available for analysis (Malone et al., 2020). A function of a machine learning system can be: descriptive, showing how the system uses the data to clarify what happened; predictive, in the way it uses the data to predict what will happen; or prescriptive, meaning that the system will use the data to make suggestions about taking action.

The application of AI/ML is changing client experiences, including identity recognition, communication channels with service providers, and investment habits. For example, automated robot advisors or "chatbots" allow for rapid and effective responses to customers and the AI/ML systems help companies to do business faster and increase overall productivity. The learning process is a critical component of most AI systems and it takes the form of ML based on mathematics, statistics, and decision theory. The improvements in ML and especially in deep learning algorithms are responsible for most of the recent achievements, such as self-driving cars, digital assistants and facial recognition (Boukherouaa et.al, 2021).

AI/ML technologies could be very beneficial as having the potential to create new jobs and increase financial inclusion through providing digital financial services such as easier access to credit. Given the growing importance of risk management in banking, AI/ML has the potential to support any risk mitigation measures providing the banks adopt adequate strategies and implementation plans (Milojević and Redžepagić, 2021). Accordingly, the carefully measured and well-prepared application of AI/ML can produce positive effects on the following risk management areas: credit, market, liquidity as well as operational risks and other related areas. On the other hand, there are weaknesses. The greater the adoption and usage of AI/ML, the greater the potential for cyber threats and attacks. Apart from traditional cyber threats caused by human or software failures, AI/ML systems are vulnerable to new threats including those focused on manipulating data at some stage of the AI/ML lifecycle (Boukherouaa et al., 2021). As the authors argue, they aim at abusing inherent limitations of AI/ML algorithms thereby enabling attackers to evade detection and cause AI/ML to make the wrong decisions or to extract sensitive information. The growing complexity of AI/ML and

the potential to affect financial stability requires constant monitoring to ensure timely detection of these risks and to prevent cyberattacks.

As the authors Prenio and Yong (2021) notice, several financial authorities have initiated the development of new governance frameworks regarding these technologies. This includes the convergence of general guiding principles regarding reliability, accountability, transparency, fairness and ethics as well as data privacy, third-party dependency and operational resilience. Such high-level principles are useful in providing a broad indication of what firms should consider when using these technologies. Nonetheless, it is still essential that financial regulators also provide concrete practical guidance.

International cooperation is both inevitable and crucial to tackle the shortcoming of AI/ML. In order to ensure that humanity as a whole benefits from the development of artificial intelligence and that weaknesses of the latter are properly recognized and managed, the report entitled "Recommendation on the Ethics of Artificial Intelligence" was adopted by the UNESCO General Conference at its 41st session on 24 November 2021 (UNESCO, 2021). According to the report, these technologies could be beneficial to the environment and ecosystems. However, in order to ensure the realization of benefits, any potential harm should be actively resisted and not ignored.

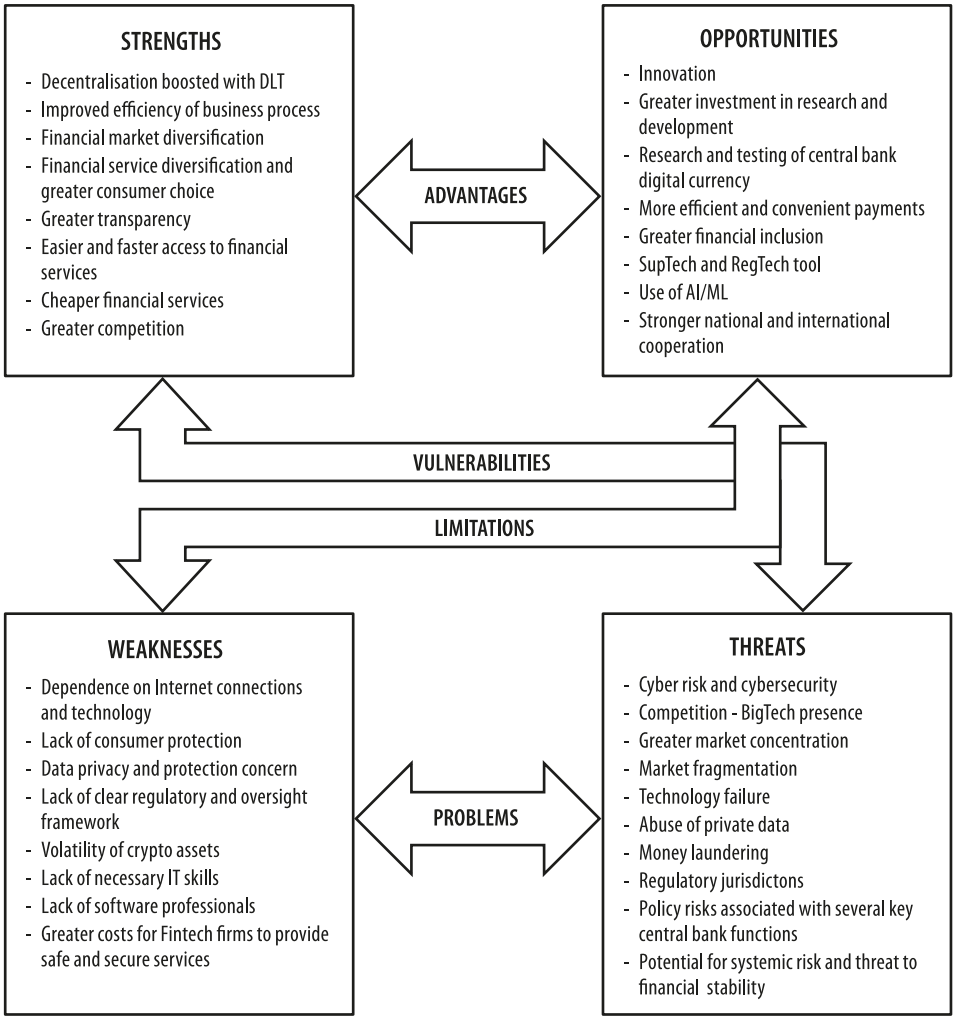
Even though developing economies can benefit from AI/ML, they are currently lagging behind because they require more research, investment and improved human capital. According to Boukherouaa et al. (2021) the use of AI/ML is greater in advanced than developing countries, which poses the threat of a deepening of the digital divide between them. In regards to the latter, they identify four broad pillars needed for bridging the gap and they include investments in: infrastructure, policies for a supportive business environment, upgrading skills and developing risk management frameworks.

As Malone et al. (2020) point out, despite the recent major progress and development, artificial intelligence is still not close to matching the breadth and depth of perception, reasoning, communication, and creativity of people. Accordingly, AI systems are still incomplete in their ability to reason, make decisions or interact with people and objects in the physical world. In regards to the process of reshaping the future of employment related to these developments, Malone et al. (2020) emphasize that there should be a question of *Not People **or** Computers*, but rather, *People **and** Computers*. The idea is that a useful strategy is to begin by examining the tasks that make up a job and allow the computers to do the ones they can do best and let people do the ones they can do best.

2.3. Fintech SWOT Analysis

As explained in the text above, Fintech is beneficial and has great potential for creating various improvements and opportunities. However, it also brings with it a number of weaknesses and poses serious threats, as shown in Figure 1 below.

Figure 1: Fintech SWOT Analysis



Source: Authors` findings

Strengths and opportunities are advantages, while weaknesses and threats represent problems. Strengths should mitigate threats and make the system less vulnerable and more resistant to risks. For example, although DLT has the potential to boost decentralization, it can also be the source of cyber risks. To avoid the latter, it is important to make the decentralized systems more secure and increase the level of cybersecurity. Diversification of the financial market is beneficial and creates a source for greater competition. On the other hand, there is a risk that the increased presence of BigTechs could jeopardize competition and pose concentration risks.

While easier, cheaper and faster services are more convenient for users, they are also prone to privacy data breaches and the misuse of information. What's more, a significant technological failure could disrupt or even disable the use of services. It is clear from all of the above that strong cybersecurity is of exceptional importance.

Weaknesses could be limiting factors in taking advantage of opportunities so it is important to minimize them and diminish their effects. Overdependence on the Internet can negatively affect the efficiency and the speed of payments. Lack of consumer protection and data privacy issues may endanger increased financial inclusion. Lack of clear regulatory and oversight frameworks as well as insufficient IT skills could diminish the beneficial side of AI/ML.

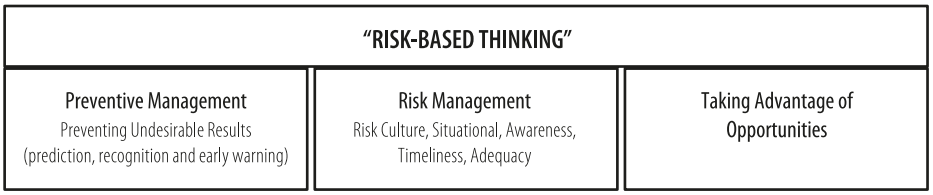
On the other hand, the further development of RegTech and SupTech contributes to stronger regulatory and supervisory contexts and decreases the weaknesses. A better system means that consumers can take more advantage of lower transactional costs and faster services without cyber risk. Therefore, Fintech firms have to accept greater expenses in order to provide safe and secure services that are fast and easy to use. The continuing lack of trained IT professionals and skilled labour is of huge importance, because only high skilled employees can guarantee security and safety to customers who expect the protection of their privacy.

3. "Risk-based thinking" in terms of Preventing Undesirable Results

Risk is the effect of uncertainty on objectives. Risk Management involves coordinated activities to direct and control an organisation with regard to risk. In times of ever greater and more complex risks, in order to survive, develop and be successful, everyone has to effectively and efficiently manage risk. The purpose of risk management is the creation and protection of value. "Risk-based thinking" is a new management concept of preventive action, with the primary goal of

preventing undesirable results and preserving the value of the organisation. The main purpose of the concept of "Risk-based thinking" is to establish preventive management, which is essential for the timely identification and elimination of both negative effects and potential risks.

Figure 2: Key Processes of "Risk-based thinking"



Source: Authors` findings

The set of requirements that in earlier international quality standards was designated by the term "preventive measures", was replaced by the management concept of "Risk-based thinking" in the standard ISO 9001:2015, *Quality Management Systems – Requirements* (ISO 9001:2015, pp. ix, 22). This concept emphasizes that an organization needs to understand its own context and identify potential risks and opportunities as the basis for planning and action, which essentially represents the application of "Risk-based thinking". The essence of this concept is the thinking itself, but not just any thinking. It is about thinking based on recognized risks, thinking based on risks that may yet appear, those that are both seen and anticipated, as well as those that are not seen, and which may never appear (Luburić and Perović, 2020a).

"Risk-based thinking" means not only thinking about risks, but also thinking about opportunities to improve and achieve sustained success. Such timely, purposeful and effective thinking about risks and opportunities generates a new system of behaviour and preventive action by employees, through constant review and improvement. The new behaviour by employees promotes, enriches and improves the existing way of working, as well as the values and culture of the organization, which to a large degree contributes to its more effective and efficient functioning. "Risk-based thinking", therefore, is of crucial importance in achieving an effective management system.

Bearing in mind that the essence of "Risk-based thinking" is thinking itself, it is necessary to point out some features of this very complex phenomenon of the human mind. People think about many things every day, but when asked what is

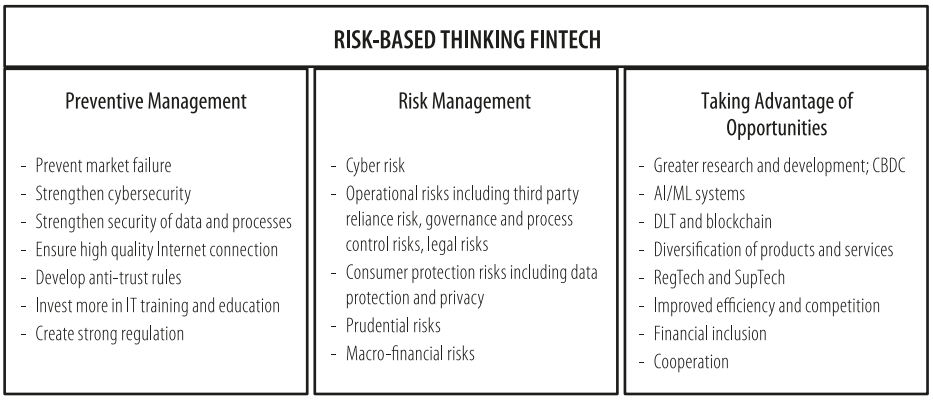
thinking, they find it difficult to explain or define. Why is that so? First, because people understand the essence and meaning of this thought process differently. In our age, the understanding of thinking, this most basic, most common and most important human activity, is very different from the times in which the generations that came before us lived. In the current conditions of dizzying technical, technological and communication innovations, many equate thinking with the mere and superficial reception and processing of information delivered to us through the numerous media and social networks. However, it is not like that (Luburić and Perović, 2020b).

Complete and comprehensive thinking is the logical, critical and mental connection and analysis of human cognition in the context of both time and space. Thinking itself is subjective and conditioned by the knowledge and experience that people possess, by their intellectual, emotional and other abilities or, in other words, through their hearts and minds. As a fundamental, timeless and permanent phenomenon of human existence, thinking is the key to understanding all phenomena and processes. All aspects of human thinking exist both interconnected and intertwined, especially the most complex. The concept of "Risk-based thinking" is, in fact, a comprehensive approach to considering any problem in specific internal and external contexts. The strength of this concept is reflected in the fact that it involves not only thinking about risks and aimed at preventing potential risks, but also it involves, at the same time, thinking about potential and desirable opportunities to improve and achieve sustained success.

By using the concept of "Risk based thinking", it is possible to carry out a SWOT analysis of Fintech and thus form the basis for taking preventive measures to minimize potential cyber risks.

Preventive management, aimed at preventing undesirable results (prediction, recognition and early warning) is important to: prevent market failures in order to mitigate spillovers to financial system, preserve financial stability, and lower the potential for systemic risks; strengthen security of data and processes; fortify cybersecurity space to provide cheaper, more efficient, and convenient payments thereby preserving financial stability and convincing people of the trustworthiness of digital financial service; ensure high quality Internet connection; develop anti-trust rules for the digital era, data mobility requirements and data protection laws; invest more in training and education of IT professionals as well as general development of digital financial technology (DFT) skills; create strong regulation to prevent money laundering, abuse of privacy issues, data concentration; and support positive competition particularly in terms of BigTech market presence.

Figure 3: Fields of "Risk-based thinking" in terms of strengthening Fintech



Source: Authors' findings

Central banks are making great efforts to prepare for the future of money, including research and testing of CBDC. The authorities are aware that it is better to prepare systems in case there is a need for issuance of CBDCs because it is more valuable than to let private companies and particularly BigTechs take over the market of digital currencies. It is obvious that BigTechs have great power primarily through data already at their disposal, as well as well-developed communication with users and a positive reputation with them. The creation of Fintech hubs where many large monetary authorities are involved is very important especially in regards to cross border payments.

Risk management is another important segment of "Risk-based thinking" which can strongly contribute to better and more secure financial technology services. Cyber risk is one of the most emphasized risks related to Fintech thus strong and adequate management of it is necessary. As the application of technology expands, the space for cyberattacks extends as well while attackers operate across borders and endanger individuals or companies both in rich and poor countries. There are other operational risks including third party reliance risk, business process control and legal risks. Consumer protection is also as important issue primarily in regards to data protection and privacy. Prudential risks are also significant and have to be controlled. Macrofinancial risks including excess volatility of Fintech services and the systemic importance of Fintech firms should be effectively managed. "Risk-based thinking" is very important in regards to AI/Ml development. Nevertheless, while the improvement and innovation of AI/ML can bring benefits in performing financial activities, that level of technology has

its weaknesses and threats. In order to minimize these, the identification of those risks and preventive measures are necessary.

Fintech should be seen as a source of opportunities as it could influence greater investment in research and development, support high quality digital financial innovations including AI/ML research especially in developing economies, support diversification of product and services, increase data security, boost transparency and contribute to financial inclusion. Adoption and implementation of RegTech and SupTech will further contribute to better risk management and allow for more sophisticated regulation and supervision of Fintech. This will have preventive effects and minimize abuse of the lack of regulation and control measures. Services provided at reduced costs, improved efficiency, greater access and financial inclusion are some of beneficial sides of Fintech. Needs for Fintech development and more coordinated policies could improve national and international cooperation.

There is a great potential to expand the use of blockchain-based technologies even further from financial services. According to European Union Agency for Cybersecurity (ENISA, 2021a) there are proposals to apply blockchain technology for electronic voting, secure sharing of medical data, as well as in the field of digital identities.

4. Cyber Risk in the Fintech Landscape

The main threat of these modern times of digital technological innovation is cyber risk. Financial services and infrastructure are especially exposed to cyberattacks due to the critical services they provide (Aldasoro, Gambacorta, Giudici, and Leach, 2020). As the authors point out, broadly speaking, cyber risk generally refers to the risk of financial loss, disruption or reputational damage to an organization resulting from the failure of its IT systems. According to Cebula and Young (2010), cyber risk includes operational risks to information and technology assets that can produce consequences to the confidentiality, availability, or integrity of information or information systems. Therefore, it is crucial to provide a safe cyber space and ensure cybersecurity.

However, cyber incidents are ever more sophisticated, while their costs are ever more difficult to measure. A widespread understanding of the damage either threatened or caused by such cyber events is essential in order to ensure coherent, adoptable and durable cybersecurity capacity-building around the world (Agrafiotis et al., 2016). The authors also advocate that by definition, cyber damage

is the harmful consequences resulting from cyber events, which can originate from malicious, accidental or natural phenomena, manifesting itself either within or outside of the Internet. Therefore, in order to build a relevant and efficient cybersecurity capacity and for such efforts at harm reduction and avoidance to be reliable, a complete understanding of the sources, scale and consequences of potential cyber harm is indispensable. The intensified use of new financial technology during the Covid-19 pandemic has further increased the potential for cyberattacks. As a result, cybersecurity risk has become one of the top three risks for Fintech in the light of Covid-19 (CPMI-WB, 2020). Assessments are that large cyberattacks present a real threat to financial stability and that it is not a question of whether it will happen, but rather when it will happen (Fabris, Luburić and Sekulović, 2021).

The interconnected world is ever more prone to cybersecurity failures and cybercrime. Due to the extensive dependency on more complex digital systems, cyber threats are outperforming the current potential to successfully prevent and manage them. Cyberattacks themselves are becoming more widespread, sophisticated and destructive. In the fight against cyber risk, preventive action is of special importance, as well as the maturity and readiness of the entire society to face this dangerous challenge (Fabris et al., 2021). Response strategies consist of reviewing disaster recovery plans, establishing crisis management, and developing communication plans. Thereby, the establishment and continual development of a culture of cyber security is of invaluable importance.

Aldasoro et al. (2020) state that cyber costs are higher for bigger firms and for incidents that affect several organizations simultaneously. Although the financial sector faces a larger number of cyberattacks, it suffers lower costs on average because of the proportionately greater investment in information technology security. The use of cloud services comes with lower costs, particularly when cyber incidents are relatively small, however, as cloud providers become systemically important, cloud dependence is likely to increase tail risks (Aldasoro et al., 2020). All crypto-related activities are particularly vulnerable to cyberattacks.

According to the Allianz Risk Barometer (Allianz Global Corporate & Specialty–AGCS, 2022a), which is an annual report identifying the top corporate risks for the next 12 months and beyond, based on the views of more than 2,650 risk management experts from 89 countries and territories, cyber threats are considered the largest concern for companies globally in 2022. In regards to the latter, the report showed that the ransomware attacks, data breaches and major IT outages worry companies even more than business and supply chain disruption, natural disasters or the Covid-19 pandemic, all of which have seriously affected firms

in the previous years. Based on the results of the report (AGCS, 2022b), 44% of respondents identified cyber incidents as the top risk in the list of the ten most important global business risks.

The Global Risks Perception Survey (GRPS) carried out by the World Economic Forum (WEF, 2022) and published in the Global Risks Report 2022 shows that "cybersecurity failure" is a critical short-term threat to the world, ranking it among the top-10 risks that have increased since the start of the COVID-19 crisis. Furthermore, 85% of the Cybersecurity Leadership Community of the World Economic Forum have emphasized that "ransomware" is becoming a dangerously rising threat and presents a major concern for public safety. Additionally, at a regional level, "cybersecurity failure" is ranked as a top five risk in East Asia and the Pacific as well as in Europe, while four countries - Australia, Great Britain, Ireland and New Zealand— ranked it as the number one risk.

Rapid digitalization in advanced economies during the COVID-19 pandemic has further increased the level of cyber vulnerabilities. According to the WEF (2022), there is a risk that concerns over cybersecurity could further hinder attempts to promote fast and inclusive digitalization globally as rapid digitalization exposes economies to new and more intense cyber vulnerabilities, as new technologies and an ever-expanding attack surface allow the creation of more dangerous and different range of cybercrimes. Sophisticated cyber tools are also letting the actors of these cyber threats identify targets of choice more efficiently, underlining the potential to carry out more goal-oriented attacks that could lead to even higher financial, societal and reputational damage in the future (WEF, 2022). There are worries that developments in quantum computing could be influential enough to break existing encryption keys, which poses a significant security risk because of the sensitivity and criticality of the financial, personal and other data protected by these keys. The development of the so-called "metaverse" could also broaden the surface for malicious attacks by generating more entry points for malware and data breaches. As the value of digital commerce in the "metaverse" increases in scope and scale and projected to be worth over US$800 billion by 2024, the potential for those attacks to cause great harm significantly increases.

According to ENISA (2021b), there was a series of cyber threats that emerged and materialized during the course of 2020 and 2021 and was the subject of an analysis entitled, Threat Landscape 2021. The latter identifies and emphases several prime threat groups that are highlighted based on their prominence during the reporting period, their popularity and the effect of their materialization Those are: ransomware (*a malicious attack where attackers encrypt an organization's data and demand payment to restore access*) which is ranked the prime

threat during the reporting period; malware (*software or firmware projected to perform an unauthorized process having an adverse impact on the confidentiality, integrity, or availability of a system*); cryptojacking (*or hidden crypto mining refers to a cybercrime when a criminal secretly uses a victim's computing power to generate cryptocurrency*); e-mail related threats (*threats that exploit weaknesses in the human psyche and in everyday habits, rather than technical vulnerabilities in information systems*); threats against data (*includes data breaches/leaks when can be released sensitive, confidential or protected data to an untrusted environment*); threats against availability and integrity (*availability and integrity are the target of threats and attacks, among which the families of Denial of Service (DoS) and Web Attacks stand out*); disinformation – misinformation (*on the rise due to increased use of social media platforms and online media*); non-malicious threats (*malicious intent is not apparent, mostly based on human errors and system misconfigurations*).

According to Fabris et al. (2021), any strengthening of cybersecurity has to begin with a full understanding of the nature of cyber risk, as without this understanding the identification of potential weaknesses and the building of an adequate defence against cyber risk is impossible. They go on to identify five key challenges in managing cybersecurity in financial systems. Those are the complexity of the further development and interconnectedness among financial institutions in various countries, the lack of well-trained staff for cyber risk management, insufficient understanding of the nature of cyber risk, increase in the digitalization of business, the expansion of financial innovation and digital assets, and further expansion of business.

Concerns about financial stability are mounting because of the digitalization of financial services and the increasing use of third-party service providers (FSB, 2021b). The latter influenced the Financial Stability Board`s examination of the harmonization of cyber incident reporting. One of the key elements of the work program of FSB refers to improving cyber resilience in order to promote financial stability. According to FSB (2021b), fragmentation exists across sectors and jurisdictions in regards to defining what actually is a cyber-incident, the methodologies used to measure the depth and impact of an incident, different timeframes for reporting cyber incidents as well as how the information about a cyber-incident is used. The latter implies that financial institutions that function across borders or sectors are subject to multiple reporting requirements for each cyber-incident, which means that financial authorities receive heterogeneous information about a particular incident that as a result could undermine its response and recovery actions. This underlines the need to address limitations in information sharing among authorities and financial institutions. Therefore better harmonization of

the regulatory reporting of cyber-incidents would promote financial stability by creating a common understanding, and monitoring of cyber-incidents that impact financial institutions and the financial system. It is essential to encourage effective cyber risk supervision in financial institutions; and facilitate the coordination and sharing of information among authorities across sectors and jurisdictions (FSB, 2021b). As Fabris et al. (2021) point out, the implementation of international cybersecurity standards is very important as well as that of domestic regulations. Financial institutions allocate significant reserves for credit, market and other risks, but to date they have not been allocating reserves for potential losses stemming from cyberattacks.

CBDC could also be an attractive field for cyberattacks. The number of cyber breaches have increased during the COVID-19 pandemic due to the increased use of IT although payment service providers were under cyberattacks both before and during the pandemic. The growing frequency of major data breaches in recent years, in particular at financial institutions, underline the possibility that data or funds may be embezzled (BIS, 2021b). Those risks would be similar for CBDC payment services. Accordingly, any identification framework requires a strong cybersecurity and while identification based on a unique digital ID is critical for the safety of payment systems and transactions in a CBDC, there is an offsetting imperative to protect the privacy and safety of users. In addition, besides simple stealing, there are combinations of transactions, geolocations, the use of social media and data search that increase concerns about data abuse and even personal safety (BIS, 2021b). In the potential retail CBDC architecture models, the level of risk to cyberattacks depends on the amount of central banks data exposed to such risks.

As long as AI/ML systems strongly influence the financial sector landscape, they can be a source of risks. As well as the various benefits AI/ML developments bring with them, they also bring significant risks due to the opaqueness of their outcomes, and their robustness, particularly with respect to cyber threats and privacy (Booukherouaa et al., 2021). The effective management of these risks and comprehensive prevention of cyber risk in the field of AI/ML is vital in order to avoid threats to numerous personal and confidential financial data breaches.

As the use of digital technology develops, the entire world is becoming potential space for cyber attackers to act. They simply act globally. It is wrong to assume that cyberattacks come from only a limited number of countries and that they could then become subject to more restrictions. In reality, cyber attackers could potentially attack from anywhere.

5. Conclusion

Fintech innovations have changed the traditional methods of delivering financial services. Faster, cheaper and easily accessible digital financial services, greater business efficiency, market diversification and decentralization as well as reshaped communication channels between financial service providers and consumers have created space for greater transparency and financial inclusion.

The presented SWOT analysis shows that apart from its beneficial side, Fintech has weaknesses and potentially poses significant threats to the financial system. Cyber risk, dependence on Internet connection, potential for data and privacy breaches, lack of legal frameworks, volatility of crypto currencies, and insufficient competition due to the great influence of BigTech, are among the disadvantageous side of Fintech. "Risk-based thinking" has to be more widely used, not only to emphasize strengths but also to mitigate risks and minimize weaknesses. Increased research and development in terms of financial innovations, taking advantage of decentralization and blockchain as well as the improved efficiency of financial services, are some of areas where "Risk-based thinking" could further strengthen the many positive features of Fintech. Preventive measures based on "Risk-based thinking" can contribute to mitigating the negative side of Fitech. They should include minimizing cyber risk, reinforcing cybersecurity, the adoption and implementation of the necessary legal framework to diminish abuse of the lack of regulation, stronger network connections, as well as better consumer protection regulation to increase the level of trust in the digital financial services.

Large cyberattacks pose a real threat to financial stability and the issue is not whether it will happen but rather when it will happen. The interconnected world is open to cybersecurity failures and cybercrime. Cyberattacks themselves are becoming ubiquitous, sophisticated and destructive. Response strategies include reviewing disaster recovery plans, establishing crisis management, and developing communication plans. Accordingly, the setting up and continual development of a culture of cyber security is of priceless importance. AI/ML can be extremely beneficial in terms of increasing financial inclusion through providing convenient and efficient digital financial services but the greater the adoption and usage of AI/ML, the greater the potential for cyber threats and attacks.

It is clear that monetary and financial authorities are making great efforts to act preventively and set up their systems for both the current and possible future market requirements. If they wait before taking action, they could potentially lose more and they should act preventively and be prepared to activate new plans and make new decisions. Of course, in all these attempts the authorities focus

on preserving monetary and financial stability. Central banks manage financial risks as well as non-financial risks including policy risks, operational and reputational risks. Being aware of the rapid developments and changes in the financial services as well as consumer preferences, central banks are making strong efforts to satisfy the needs of the market whilst staying dedicated to fulfilling their primary goals – preserving monetary and financial stability. They are committed to building innovative, inclusive, competitive and resilient payment systems including research and the potential issuance of CBDC. This has the potential to improve the efficiency of cross-border payments and bring novelty in the way central banks traditionally operate. While there are possible retail or wholesale structures of the CBDCs, they are, however, still in their infancy. Nevertheless, they call for the coordination of national CBDC designs in order to contribute to more efficient cross-currency and cross-border payments.

The rapid development of Fintech requires more oversight and supervision from regulators. Although international institutions have placed the rapid technology driven developments in financial services among the priorities in their policies, increased cooperation among authorities is important both at national and international levels. The pace of financial innovations is rapid and it will continue to accelerate, together with the increased risks from cybercrime and cyberattacks. Thus, the need for preventive actions and "risk-based thinking" is crucial and will remain so in the future.

References:

1. Agrafiotis, I., Maria, B., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., Roberts, T., Upton, D. (2016). Cyber Harm: Concepts, Taxonomy and Measurement. Saïd Business School WP 2016-23. Available at: SSRN: https://ssrn.com/abstract=2828646
2. Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T. (2020). The Drivers of Cyber Risk. BIS WP No 865. Retrieved from: https://www.bis.org/publ/work865.pdf
3. Allianz Global Corporate & Specialty (2022a). Allianz Risk Barometer 2022, Retrieved from: https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html
4. Allianz Global Corporate & Specialty (2022b). The Most Important Global Business Risks for 2022, Retrieved from: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
5. Auer, R. and Böhme, R. (2021). Central Bank Digital Currency: the Quest for Minimally Invasive Technology. BIS WP No 948. Retrieved from: https://www.bis.org/publ/work948.pdf
6. Auer, R., Frost, J., Gambacorta, L., Monnet, C., Rice T. and Shin, H. (2021). Central Bank Digital Currencies: Motives, Economic Implications and the Research Frontier. BIS Working Papers No 976. Retrieved from: https://www.bis.org/publ/work976.pdf
7. Bains, P., Sugimoto, N. and Wilson, C. (2022). BigTech in Financial Services: Regulatory Approaches and Architecture. IMF NOTE/2022/02 Retrieved from: https://www.imf.org/en/Publications/fintech-notes/Issues/2022/01/22/BigTech-in-Financial-Services-498089
8. Bank for International Settlements (2021a). BIS Appoints Innovation Hub Heads for London, Nordic and Toronto Centres. Press Release. November 30. Retrieved from: https://www.bis.org/press/p211103a.htm
9. Bank for International Settlements (2021b). CBDCs: an Opportunity for the Monetary System. BIS Annual Economic Report 2021. Retrieved from: https://www.bis.org/publ/arpdf/ar2021e3.pdf
10. Bank for International Settlements (2021c). Central bank digital currencies for cross-border payments. Report to the G20. Retrieved from: https://www.bis.org/publ/othp38.pdf
11. Bank of France, Bank for International Settlements and Swiss National Bank (2021). Project Jura. Cross-Border Settlement Using Wholesale CBDC. Retrieved from: https://www.bis.org/publ/othp44.pdf

12. Boukherouaa, B., Shabsigh, G., AlAjmi K., Deodoro, J., Farias, A., Iskender, E., Mirestean, A., and Ravikumar R. (2021). Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance. IMF. DP/2021/024
13. Cambridge Center for Alternative Finance and World Bank Group (2020). The Global Covid-19 FinTech Regulatory Rapid Assessment Study. World Bank Group and the University of Cambridge. Retrieved from: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-report-fintech-regulatory-rapid-assessment.pdf
14. Cebula, J.J. and L.R. Young (2010). A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Retrieved from: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf
15. European Central Bank (2021a). Eurosystem Launches Digital Euro Project. Press Release July 14, Retrieved from: https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html
16. European Central Bank (n.d). Digital Euro. Retrieved from: https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html (Accessed on March 3, 2022)
17. European Union Agency for Cybersecurity (2021a). Can Digital Identity Solutions Benefit from Blockchain Technology?. Retrieved from: https://www.enisa.europa.eu/news/enisa-news/can-digital-identity-solutions-benefit-from-blockchain-technology
18. European Union Agency for Cybersecurity (2021b). ENISA Threat Landscape 2021. Annual Report. ENISA. Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
19. Fabris, N. (2018). Challenges for Modern Monetary Policy. *Journal of Central Banking Theory and Practice*, 7(2), 5-24. Available at: DOI: 10.2478/jcbtp-2018-0010
20. Fabris, N., Luburić, R. and Sekulović, R. (2021). Sajber Rizik u Finansijskom Sistemu - Izazovi Tokom Pandemije Koronavirusa. *Sistem kvaliteta uslov za uspešno poslovanje i konkurentnost*. pp. 27-37
21. Feyen, E., Frost, J., Gambacorta, L., Natarajan, H. and Saal, M. (2021). Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy, BIS WP No 117. Retrieved from: https://www.bis.org/publ/bppdf/bispap117.pdf
22. Financial Stability Board (2020a). The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions. FSB. Retrieved from: https://www.fsb.org/wp-content/uploads/P091020.pdf

23. Financial Stability Board (2020b). Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements. Final Report and High-Level Recommendations. FSB. Retrieved from: https://www.fsb.org/wp-content/uploads/P131020-3.pdf
24. Financial Stability Board (2021a). Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements. FSB. Retrieved from: https://www.fsb.org/wp-content/uploads/P071021.pdf
25. Financial Stability Board (2021b). Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence. Retrieved from: https://www.fsb.org/wp-content/uploads/P191021.pdf
26. Financial Stability Board (n.d). Fintech. Retrieved from: https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/fintech/ (Accessed on March 1, 2022)
27. International Monetary Fund (2018). The Bali Fintech Agenda: A Blueprint for Successfully Harnessing Fintech's Opportunities. Press Release No 18/388. Retrieved from: https://www.imf.org/en/News/Articles/2018/10/11/pr18388-the-bali-fintech-agenda
28. ISO 9001:2015, Quality management systems – Requirements, International Organization for Standardization, Geneva, Switzerland 2015.
29. Khan, A. and Malaika, M. (2021). Central Bank Risk Management, Fintech, and Cybersecurity. IMF WP/21/105. Retrieved from: https://www.imf.org/en/Publications/WP/Issues/2021/04/23/Central-Bank-Risk-Management-Fintech-and-Cybersecurity-50278
30. Luburić, R. and Perović, M. (2020a). Risk-based thinking in terms of strengthening Quality Management Principles, *Kvalitet & Izvrsnost*, 2020, 7-8, pp. 15-18. Retrieved from: https://www.researchgate.net/publication/344250757
31. Luburić, R. and Perović, M. (2020b). Risk-based thinking as a new concept of preventive management, *Kvalitet & Izvrsnost*, 2020, 9-10, pp. 24-29. Retrieved from: https://www.researchgate.net/publication/345309498
32. Malone, T., Rus, D. and Laubacher, R. (2020). Artificial Intelligence and the Future of Work, Massachusetts Institute of Technology. Retrieved from: https://workofthefuture.mit.edu/wp-content/uploads/2020/12/2020-Research-Brief-Malone-Rus-Laubacher2.pdf
33. Milojević, N. and Redžepagić, S. (2021). Prospects of Artificial Intelligence and Machine Learning Application in Banking Risk Management. *Journal of Central Banking Theory and Practice*, 10(3), 41-57. Available at: DOI: 10.2478/jcbtp-2021-0023

34. Panetta, F. (2020). From the payments revolution to the reinvention of money, Speech by Member of the Executive Board of the ECB, Frankfurt am Main. Retrieved from: https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp201127~a781c4e0fc.en.html
35. Prenio, J. and Yong, J. (2021). Humans keeping AI in check – emerging regulatory expectations in the financial sector. FSI Insights on policy implementation No 35. BIS. Retrieved from: https://www.bis.org/fsi/publ/insights35.htm
36. Soderberg, G., Bechara, M., Bossu, W., Che, N., Kiff, J., Lukonga, I., Mancini-Griffoli, T., Sun, T., and Yoshinaga, A. (2022). Behind the Scenes of Central Bank Digital Currency, Fintech Notes. IMF NOTE/2022/004.
37. UNESCO (2021). Report Of The Social And Human Sciences Commission (SHS)41 C/73 22 November 2021, Retrieved from: https://unesdoc.unesco.org/ark:/48223/pf0000379920.page=14
38. Vučinić, M. (2020). Fintech and Financial Stability Potential Influence of Fintech on Financial Stability, Risks and Benefits. *Journal of Central Banking Theory and Practice*, 9(2),43-66, Available at: DOI: 10.2478/jcbtp-2020-0013
39. World Economic Forum (2022). The Global Risk Report 2022. Retrieved from: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf