European Commission

April 2021

# Advanced Technologies for Industry - Sectoral Watch

*Technological trends in the financial services and the banking sector*

This report was prepared by Patrick de Bas, Priss Zhou and Sem Enzerink from Capgemini and Kincsö Izsak from Technopolis Group.

**EUROPEAN COMMISSION**

European Innovation Council and SMEs Executive Agency (EISMEA)

Unit I-02.2 SMP / COSME Pillar

E-mail: EISMEA-COSME-ENQUIRIES@ec.europa.eu

Directorate General for Internal Market, Industry, Entrepreneurship and SMEs

Unit D.2 — Industrial forum, alliances, clusters

E-mail: GROW-ATI@ec.europa.eu

European Commission

B-1049 Brussels



PDF ISBN 978-92-9460-439-2 doi: 10.2826/224127 EA-08-21-010-EN-N

# Table of contents

Section

# Introduction

This sectoral report has been prepared in the framework of the 'Advanced Technologies for Industry' (ATI) project, initiated by the European Commission, Directorate General for Internal Market, Industry, Entrepreneurship and SMEs and the European Innovation Council and SMEs Executive Agency.

It analyses trends in the generation and uptake of advanced technologies, as well as related entrepreneurial activities and skills needs in the financial services and banking sector. It interprets data from a list of data sources, compiled to monitor advanced technologies and their applications in industry across Europe and key competitor economies.

The starting point of this analysis has been 16 advanced technologies that are a priority for European industrial policy, which enable process, product and service innovation throughout the economy and hence foster industrial modernisation. 'Advanced technologies' are defined as recent or future technologies that are expected to substantially alter the business and social environment, and include advanced materials, advanced manufacturing, artificial intelligence, augmented and virtual reality, big data, blockchain, cloud technologies, connectivity, industrial biotechnology, Internet of Things, micro- and nanoelectronics, mobility, nanotechnology, photonics, robotics, and security.

The relevance of these specific technologies in the financial services and banking sector has been explored through patent analysis and data on private equity investments, skills and technology uptake. The full methodology behind the data calculations is available here: https://ati.ec.europa.eu/reports/eu-reports/advanced-technologies-industry-methodological-report.

This report is structured as follows:

1. The first section sets the industrial context.
2. The second section analyses technological trends in advanced technologies applied in the financial services and banking sector.
3. The third section presents findings about private equity investment and start-up/spinoff activity in the area of financial technology (FinTech).
4. The fourth section explores the supply and demand of skills related to advanced technologies in financial services and banking.
5. The fifth chapter concludes with a short future outlook.

Section 1

# 1. Setting the scene: industrial context

**Key messages**

The financial services and banking sector has gone through a period of **significant changes** over the last few decades, including a global financial crisis. The dynamics of the banking market is also visible in the recent patterns of **employment**. Various developments, including digitalisation, has led to an overall decline in employment.

Industrial recovery in response to the COVID-19 pandemic will be based on advanced and disruptive technologies. **Artificial Intelligence, Blockchain and Robotic process automation** are able to enhance overall sectoral performance, mainly by improving customer experiences and reducing operational costs. **Cybersecurity** will remain an operational priority, as the further uptake of advanced technologies in finance is expected to increase the level of cyber threats.

Digitalisation, and Cybersecurity in particular, is expected to further shift labour demand and will require **reskilling the banking workforce**.

## 1.1 Sectoral changes

A financial service sector offers financial goods. The financial sector covers many different types of transactions in such areas as real estate, consumer finance, banking and insurance. It also covers a broad spectrum of investment funding, including securities.[1] In this study, the primary focus lies on the banking.

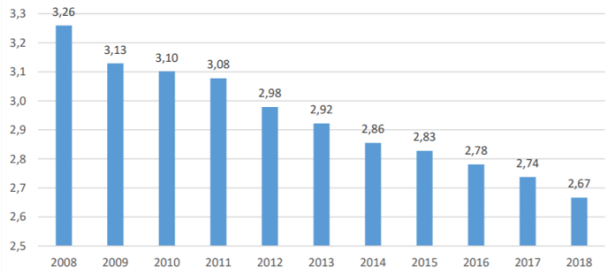
The financial services and banking sector has gone through a period of significant changes over the last few decades. European banks have been hit hard by the 2008/09 global financial crisis. Following this crisis, many countries in the world underwent significant financial sector reform to reduce or eliminate distortions in financial markets and strengthen financial institutions.[2]

Changes in the sector are also reflected in the number of banks (or credit institutions). with the number falling to 6 088 institutions. Between 2009 and 2018, 29% of the credit institutions disappeared, leaving a total of 6 088 institutions remaining in 2018.[3]

## 1.2 Banking services employment

Banks have a large stake in society as important job creators. However, due to automation, digitalisation and process optimisation, the workforce of the banking industry has steadily dropped in the last decade. Overseeing 10 years, one fifth of the 2.7 m people employed in the sector in 2008 were no longer part of the sector in 2018.[4]

*Figure 1: Number of employees in credit institutions (in millions)*




*Source: European Banking Federation, 2019*

Besides the employment decline, the banking profession itself is changing. In the light of digitalisation, and cybersecurity developments in particular, banks gradually turn into IT-orientated companies. Although some traditional banking skillsets remain to be relevant (e.g. traders, customer care), more novel professions have entered the banking institutions rapidly and take over core activities (e.g. software developers, technical architects and data scientists capable of working with Artificial Intelligence).[5]

## 1.3 Advanced technologies in the financial services and banking sector

Looking towards recovery from the financial crisis in the form of future growth, the banking sector experiences several drivers of change (see Figure 2).

[1] IMF, 2020.
[2] WTO, 2020.
[3] EBF, 2020c.
[4] EBF, 2020c.
[5] EBF, 2020a.

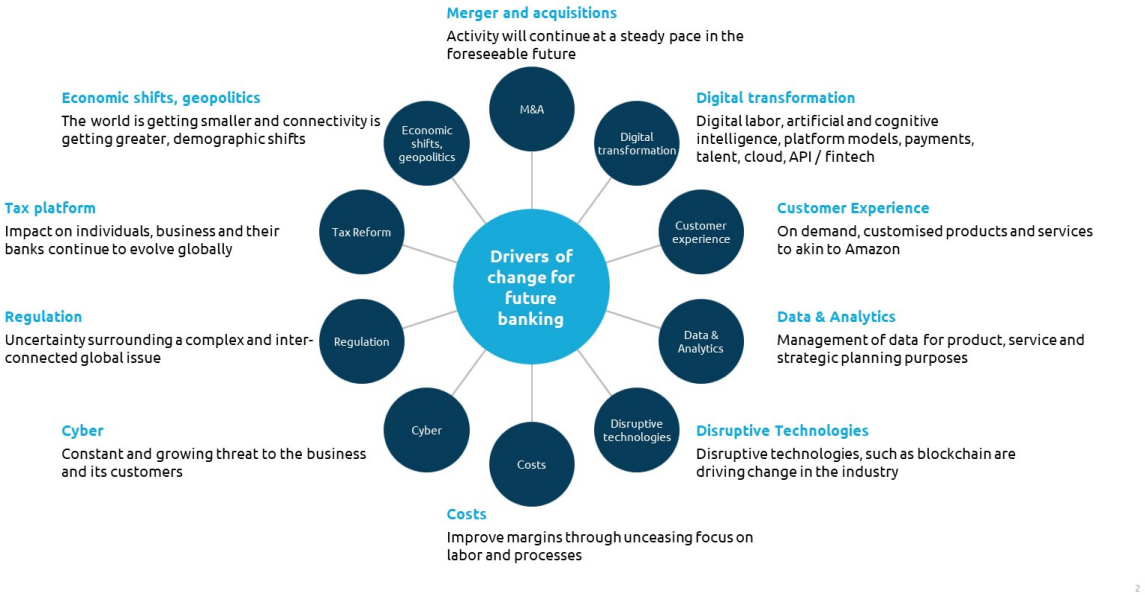
For this study, the most interesting, advanced technologies that drive the sector forward are:

- Artificial Intelligence (digital transformation)
- Blockchain (disruptive technologies)
- Robotic process automation (digital transformation)
- Big Data (data & analytics)
- Cloud (digital transformation)
- Cyber (security)

**Digital transformation and disruptive technologies** are changing the nature of the financial system, modifying the service offerings, and challenging the dominance of traditional distribution channels.

Banks have always been at the forefront of enterprise **Cybersecurity**. Their enormous stores of cash have shifted into massive amounts of consumer data and online transactions. These have made them a top target for hackers. The threat of financial losses, regulatory consequences and reputational damage has spurred them to innovate and accelerate the field of Cybersecurity.[6] Out of the data breaches in 2018, 10% of the breach victims are from the financial industry.[7] Other research found that banking and financial institutions were the most vulnerable to getting hacked.[8]

*Figure 2: Top 10 Drivers of change in the banking sector*




*Source: adapted from KPMG,2018.*

[6] BitSight, 2019.
[7] Verizon, 2020.
[8] Positive technologies, 2018.

Section 2

# 2. Technological trends

**Key messages**

The most important disruptive technologies within financial services and banking are **Artificial Intelligence, Blockchain, and Robotic process automation**. These technologies will **decrease operational costs** and **improve customer experience**.

Cybersecurity aims to reduce risks. Latest developments, such as increased usage of mobile apps, breaches at third-party organisations and increased risk of cryptocurrency hacks pose **new cybersecurity threats** for the banking sector. At the same time, advanced technologies such as Artificial Intelligence offer **new ways to counter cybercrime.** Adoption of innovative cybersecurity solutions helps the banking sector to prevent incidents as well as to trace, mitigate and resolve cybercrime after an incident.

## 2.1 Technology shifts and advances – emergence of advanced technologies, computing and software technologies

Among the most important advanced technologies within financial services and banking are Artificial Intelligence (empowered by Big Data), Blockchain and Robotic process automation.[9]

The main driver for **Artificial Intelligence** is the potential for cost savings. The most visible way the banking industry uses Artificial Intelligence is customer service supported by chatbots and robots. In the US, many of the largest financial institutions, such as Bank of America and JPMorgan Chase, use Artificial Intelligence to streamline customer service. In Europe, Artificial Intelligence is used by many banks, including, for example, Deutsche Bank and ING [10,11,12]. Artificial Intelligence is also instrumental in the way financial institutions enhance security and prevent and detect fraud. The technology helps financial institutions with risk management and lending decisions and is foundational in making other technologies such as Big Data analytics and voice interfaces work.

The aggregate potential cost savings for banks from Artificial Intelligence applications is estimated at €366 bn ($447 bn) by 2023, with the front and middle office accounting for €340 bn ($416 bn) of that total.[13]

**Blockchain** is, according to the Harvard Business Review, expected to disrupt banks the way the internet disrupted media.[14] Blockchains are transparent, highly secure, and are relatively cheap to operate. As a result, they offer a wide range of advantages for financial institutions, such as:

- Reduced costs – the technology is projected to globally save the institutions around €12-16 bn in infrastructure cost alone by 2022.
- Faster transactions – instead of the typical 1-3 days needed for verification of fund transfers, Blockchain allows verification within minutes or hours.
- Improved security – the faster transactions leave less time for an intruder to intervene and divert payments or even capture transaction details.
- Improved data quality – banking data exists in multiple places with different parties able to change information. This means an increased risk of incorrect data being recorded. Blockchain will reduce the risks of data wrongfully being altered.

The banking sector is currently one of the top investors by industry in **Big Data** and business analytics solutions.[15] The financial sector can draw upon a wide range of data sources, such as payment data and other financial transactions, and personal financial information, such as mortgages and loans. Information obtained from these data can be used to optimise the customer experience and to streamline internal processes and reduce risks. In addition, information obtained from Big Data will allow financial institutions to reduce fraud. As such, Big Data forms a source for significant business improvement and is a basis for obtaining a competitive edge.

[9] Forbes, 2019
[10] Financial times, 2018a.
[11] ING, 2017
[12] Deutsche Bank, 2019.
[13] Business insider, 2019.
[14] Asia Blockchain Review, 2019.
[15] IDC, 2020.

**Robotic process automation** is used to reduce labour cost and to minimise errors. This allows Robotic process automation to both improve the customer experience as well as reduce operational costs. The primary use of this technology is to automate parts of the claims-handling processes in insurance.

In addition to improving the customer experience and reducing operational costs, Robotic process automation can also be used to improve internal processes. For example, internal approvals on transactions with low exposure, such as consumers requesting a credit card or even a mortgage, may be provided by Robotic process automation instead of human intervention. This allows financial institutions to save money, while at the same time further improving customer experience with lower overall handling times.

Finally, Robotic process automation is able to improve compliance. By standardising and automating procedures, banks can follow the many rules present in the financial sector and limit fines caused by human errors.

The revenue from Robotic process automation in financial services and banking is expected to exceed $1 bn (€0.82 bn) globally by 2023.[16]

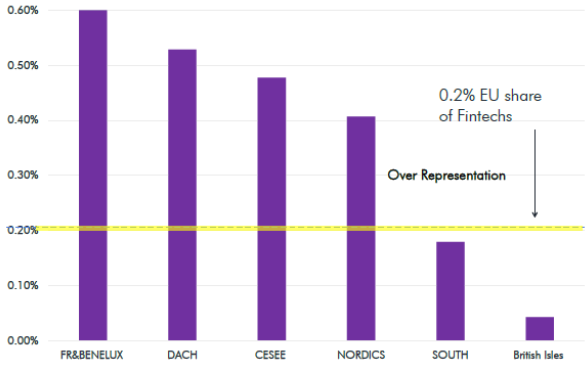
## 2.2 Technology patenting and adoption in the financial and banking sector

With respect to financial technology (FinTech[17], or digital finance), the main clusters for granted patents in FinTech are:[18]

- Trading, for example, in stocks, commodities, derivatives or currencies
- Crypto-Currencies
- Financial Security, e.g. Blockchain
- Electronic or mobile payments
- Banking, e.g. interest calculation, credit approval, mortgages
- Investments, e.g. financial instruments or portfolio and fund management
- Insurance, e.g. risk analysis or pensions

Although it is predominantly US companies who are investing in FinTech innovations, there are also European companies holding a patent portfolio in FinTech. In Europe, Barclays is the leader, with 160 FinTech patents to its name in 2017 (compared to 2 547 patents for the Bank of America)[19]. No detailed information on number of FinTech patents per firm in Europe is available.

*Figure 3: Share of FinTech within IT/Financial services (NACE J-K)*




*Source: EIB institute, 2019.*

*Note: FR&BENELUX: Belgium, France, Luxembourg, Netherlands; DACH: Austria, Switzerland, Germany; CESEE: Bulgaria, Czech Rep, Estonia, Croatia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, Slovenia, Cyprus; NORDICS: Denmark, Finland, Norway, Sweden; SOUTH: Greece, Spain, Italy, Malta, Portugal; British Isles: Ireland, UK*

As can also be observed from this list of names, banks own much less FinTech patents than other players in the FinTech space. For example, the total number of granted and pending patents for banks was 4 697 globally in 2017, much less than large technology companies IBM (23 854), Google (9 757) and Microsoft (19 670).[20] The stark difference reflects fundamentally different business strategies. Technology companies understand the role of intellectual property to define and protect markets. This is all relatively new to the financial services sector.

With the aim to examining the role of advanced technologies in shaping industrial transformation in Europe, the Advanced Technologies for Industry (ATI) survey was conducted between September and November 2020[21]. This survey investigated the uptake of advanced technologies, including their level of adoption, the associated industry-specific use cases, the digital transformation drivers that are sustained by these technologies, their expected business impacts as well as the enabling conditions.

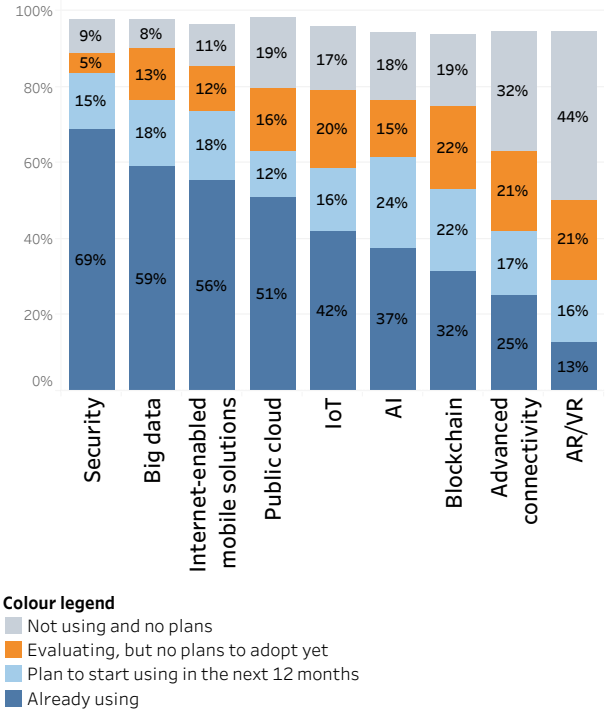
Organisations active in the financial sector were surveyed about their use of advanced

[16] Juniper, 2018.
[17] FinTech encompasses digital solutions for payments, banking, investing, mortgages and lending, financial management solutions, insurance and cryptocurrency/blockchain.
[18] Minesoft, 2020.
[19] Financial Times, 2018b.
[20] Figures for the EU were not available.
[21] The Advanced Technologies for Industry Survey sample consisted of 1 500 interviews of European organisations with more than 10 employees in Denmark, France, Germany, Italy, Poland, Spain and Sweden.
The survey was carried out between September and November 2020 and interviews were conducted through a web-based platform (CAWI – Computer-Aided Web Interviews), as well as via a Computer-Aided Telephone Interviewing (CATI) system. Additional information on survey methodology can be found in the Advanced Technologies for Industry Survey - Methodological Report available here: https://ati.ec.europa.eu/reports/eu-reports/advanced-technologies-industry-methodological-report

technologies. The survey found that 69% of the financial institutions have adopted Cybersecurity. 59% apply Big Data, 56% Internet-enabled Mobile Solutions and 51% use Public Cloud.

Artificial Intelligence has been adopted by 37% and Blockchain by 31% of organisations.

*Figure 4: Advanced technology uptake in the financial sector, 2019*




*Source: ATI Survey, 2020*

## 2.3 Technology shifts and advances – Cybersecurity

Security has traditionally been an operational priority for the banking industry. Banks initially focused on securing their vaults to protect money, gold and other stored valuables from being stolen. Nowadays, banks are shifting their focus more and more to cybersecurity to make sure consumer data and financial systems are safe too. In fact, banking and financial institutions are considered to be among the most vulnerable sectors for getting hacked and threatened by cyberattacks.[22]

The European Banking Federation estimated that Europe witnessed about 4 000 ransomware attacks per day in 2019.[23] Not only the frequency of cybercrime attacks is tremendously high, but the damage caused by cybercrime in banking is substantial too. Given the linking pin role of the financial sector, cyber risk is a danger which has the potential to trigger a systemic crisis, affecting various other sectors. The financial sector is consistently flagged as a priority by the cybersecurity community, because the continuation of services (such as online banking) and maintaining the bank's reputation and integrity is of paramount importance to ensuring cyber resilience and the smooth running of the economy.[24]

In 2018, financial damage caused by cybercrime has been estimated to be up to €536 bn for the global economy.[25] Cyber-attacks are expected to cost even €5.3 tn in 2021 globally.[26] More specifically, the banking industry has been the sector with the highest annual cost of cybercrime for several years now, already exceeding €14 m in 2018 (i.e. more than double the cost for the public sector).[27] To give a more concrete example: phishing related theft for internet banking added up to €4 m in the Netherlands alone in 2019 due to advanced and large-scale fraud.[28]

As shown in Figure 4, most incidents and breaches were caused by **social engineering techniques** (e.g. phishing) **and hacking attacks** (e.g. use of stolen credentials).[29] According to the European Banking Federation, 98% of the 2019 cyberattacks relied on social engineering techniques with vulnerabilities caused by humans.[30]

Keeping individual users secure is difficult as banking institutions have little control over their behaviour.[31] What banking institutions can do in relation to user behaviour is imposing strict security requirements and controls, such as requiring strong passwords and implementing 2 factor authentications. Customers are changing their financial behaviour and the tools with which they access and manage their finances. Financial technology solutions are now emerging as the standard way for consumers to interact with financial service providers.

Altogether, 58% of customers in the EU now regularly use digital online solutions such as websites or applications to carry out financial transactions.[32] While this has represented a leap in usability and accessibility of financial services for customers and financial service providers alike, this development also entails some risks. Customers are not necessarily proficient users of these services and a lack of technical knowledge and experience may make them vulnerable to attacks by cybercriminals deploying phishing techniques and malware solutions in order to gain

[22] Positive technologies, 2018.
[23] EBF, 2020b.
[24] ECSO, 2020.
[25] European Systemic Risk Board, 2020.
[26] Cybercrime Magazine, 2017.
[27] Accenture, 2019.
[28] NVB, 2020.
[29] Verizon, 2020.
[30] EBF, 2020b.
[31] Attila Security, 2019.
[32] Europol, 2020.

access to online accounts. On the side of the financial services, increasing digitalisation and less direct interaction with customers has the potential to weaken know-your-customer (KYC) procedures, which were put in place to prevent tax fraud, money laundering and using the financial system to finance crime and terrorism.

A discouraging but realistic message seems to be that more harmful cybercrime is yet to come. In times of the COVID-19 pandemic and social distancing, the banking sector and their clients are facing new challenges and increasing cybersecurity threats lurk. According to ENISA, phishing attacks have spiked more than 600% as per the end of February 2020.[33] Banks and their clients (both retail and corporate) are at risk while hackers commit their cybersecurity attacks, taking advantage of the chaos caused by the health crisis.

Cyberattacks have become more refined, personal and large-scale.[34] Criminals are also using advanced technologies, like Artificial Intelligence. The strong increase of banking on the web has also provided additional risks. The three risks are the use of mobile apps, breaches at third-party organisations and increased risk of cryptocurrency hacks.[35] For mobile apps, Accenture conducted an assessment of mobile banking apps, finding 2% of the apps having high level security issues and 10% medium security issues.[36]

To combat cybercrime, banks make use of **technical measures**. Institutions have more control over their own infrastructures. In particular for web portals and applications, banking institutions are able to implement monitoring and blocking technologies. Advanced technologies, used for saving costs and improving operations, also boost cybersecurity.

Fraud management systems that monitor real-time or near real-time data of customers and work using Artificial Intelligence and machine learning, have also proven successful in fighting cyberattacks.[37] Other measures include biometric identification systems, using live images and electronic signatures, inter alia to combat 'deep fake' crimes, where fake video and audio is used to impersonate clients.[38] The best fraud prevention measures are those that harness multiple layers of protection.[39] This also includes flanking measures consisting of training of the workforce, allowing corporate-client consultants to verify the payment orders with the customers and enable them to recognise attacks on their companies on their own at an early stage.[40]

However, experiences from the past have shown that technical measures alone are not sufficient to prevent cybercrime. Employee behaviour is one of the major risks associated with vulnerability of banking systems.[41] While losses from technical, software-led type of cyberattacks can be severe, such attacks are mitigated by putting in place the right kind of – layered, robust and effective – holistic cyber security programme.[42] This includes the governance structure, a cultural shift, process improvement, staff training and awareness and technology controls.

### 2.4 Technology adoption for Cybersecurity

In terms of cybersecurity market segments, information security spending is expected to grow 2.4% to reach €100 bn ($123.8 bn) in 2020 according to Gartner.[43] Two trends are worth mentioning. According to Gartner, the coronavirus pandemic is driving short-term demand in areas such as cloud adoption, remote worker technologies and cost saving measures. In addition, Gartner expects cybersecurity to be negatively impacted by the COVID-19 crisis.

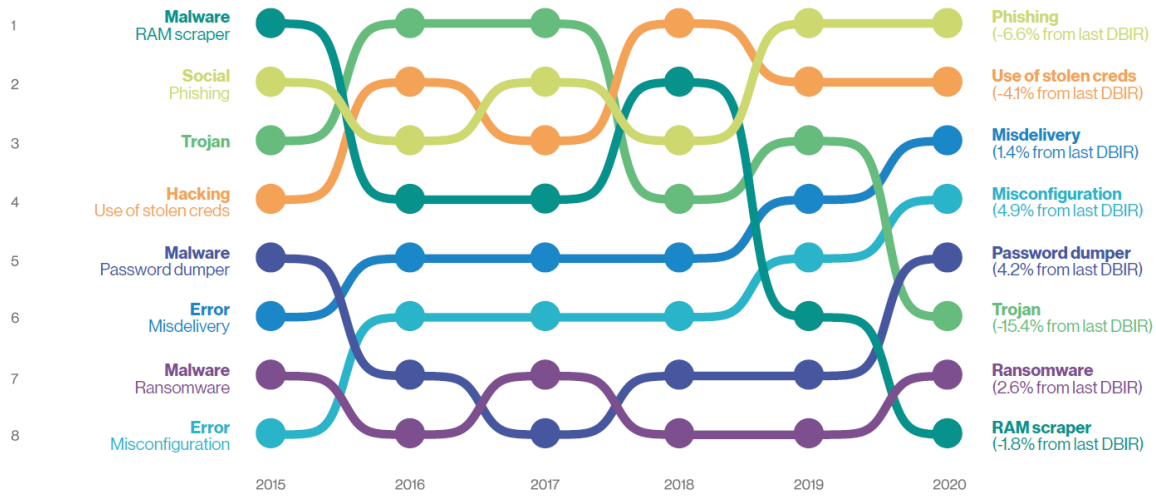
The potential halt in the growth of consumer security software could be worrisome for the banking sector. Whenever this fuels threats that target consumers (e.g. malware and ransomware), cybercrime rises with substantial costs for banks.

Turning to key application areas, Europe finds itself often in a dependent role in the global market. According to the European Economic and Social Committee, European industries are reliant on externally developed technologies (software, hardware and services). Most software and hardware are built outside the EU. The biggest global suppliers and companies managing data flows originate from the United States and China's role is rapidly expanding. Due to fragmentation and the absence of large-scale European-grown technologies, EU risks becoming excessively dependent on ICT produced outside its borders, as well as on security solutions developed elsewhere.[44] Countries like Germany, France and the Netherlands are considered to have relatively

[33] ENISA, 2020.
[34] NVB, 2020.
[35] The Global Treasurer, 2019.
[36] Figures for Android OS, for iOS OS, zero percent of the apps had high level risks and four percent has medium level risks. Source: Accenture, 2017.
[37] CIO.com/Economic Times, 2020.
[38] Chase, ABN Amro, Caixa Bank, Mastercard and Anna Money are among those that have incorporated Mitek's biometric checks. Source: Financial Times, 2020.
[39] PYMNTS.COM, 2020.
[40] International Banker, 2020.
[41] TNO, 2020.
[42] Deutsche Bank, 2016.
[43] Gartner, 2020.
[44] European Economic and Social Committee, 2018.

large and competitive markets, supported by strong regulation by national authorities, with important role played by and strong capacities of the public authorities.[45] Strong cybersecurity markets with less dependencies may help financial districts to protect banking institutions in the long term.

*Figure 5: Varieties in breaches cause over time*




*Source: Verizon, 2020. Data Breach Investigations Report (DBIR)*

*Table 1: Worldwide cybersecurity spending by segment (in million euro)*

| Market | 2019[1] | 2020[1] | Growth (%)[2] |
|---|---|---|---|
| Application security | 2 727 | 2 935 | 6.2 |
| Cloud security | 387 | 522 | 33.3 |
| Data security | 2 346 | 2 546 | 7.2 |
| Identity access management | 8 668 | 9 294 | 5.8 |
| Infrastructure protection | 14 556 | 15 610 | 5.8 |
| Integrated risk management | 4 014 | 4 224 | 3.8 |
| Network security equipment | 11 796 | 10 441 | -12.6 |
| Other information security software | 1 944 | 2 029 | 3.1 |
| Security services | 54 612 | 57 384 | 3.7 |
| Consumer security software | 5 511 | 5 567 | -0.3 |
| **Total** | **106 559** | **110 552** | **2.4** |

*Source: Gartner, 2020.*

*[1] USD/Euro exchange rate of 01/07/2019 (1.1349) and 01/07/2020 (1.1200) used for the conversion into euros.*

*[2] Growth rate excluding exchange rate effects.*

[45] Enterprise Ireland, 2019.

Section 3

# 3. Private equity investment and startup creation

**Key messages**

Within the EU27, **Germany has attracted the largest venture capital (VC) investment in FinTech** in the period 2015-2020, followed by Sweden and France. Half of the investment went into ten FinTech firms from Germany, Sweden, France, Ireland, Netherlands and Latvia. A key issue for EU FinTech financing is the lack of large ticket size investments that hinder companies to scale up.

Internationally, **VC and private equity investment into FinTech is led by the US**, nevertheless China and the EU27 perform better when looking at the average funding amount per company. Both US and Chinese VC investment is concentrated into a handful of FinTech firms.

The largest FinTech startup hubs are located in **Germany, Spain, France, Estonia and the Netherlands.** Most of the startups focus on financial software and internet solutions. **Blockchain, cryptocurrency, bitcoin** represent the technological focus for 24% of FinTech startups, with most of the blockchain startups located in Estonia. Financial apps and mobile payment solutions are also areas that have received high interest from startups. Artificial Intelligence has been the topic of 7% of startups. Cybersecurity has a mediocre focus of the VC-backed banking services startups, likely due to substantial internal investments that are ongoing in the banking sector.

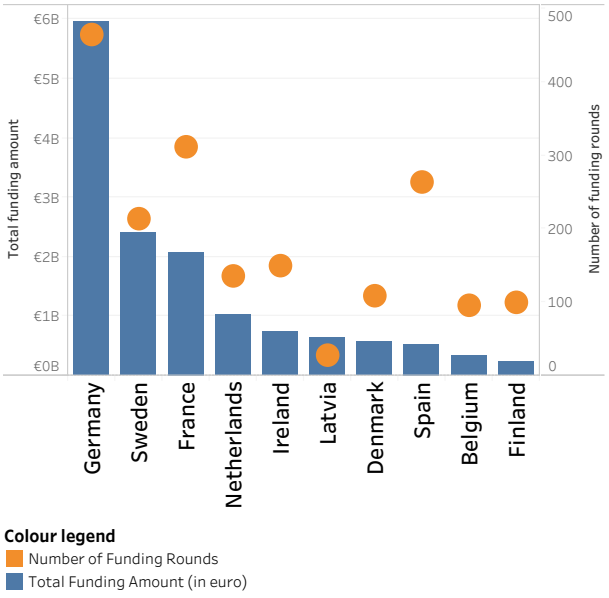
## 3.1 Private equity and venture capital investment

Venture capital (VC) investment in FinTech was tracked using a combined set of Crunchbase and Dealroom data. From the joint database, companies were selected by filtering for the 'FinTech' category and also searching in the business descriptions of companies active in Financial services. Crunchbase provides information on venture capital-backed innovative companies. Dealroom contains the same type of information but with a better coverage for Europe. The investment figures presented in this section refer only to the funding rounds where a value has been disclosed.

The analysis reveals that there are certain hotspots of VC activity in the area of FinTech innovation in Europe, such as in **Germany** that stands out with a high overall funding amount, but **also in Sweden and France** as depicted in Figure 5. A comparable picture emerges when looking at the number of funding rounds in FinTech. Most funding rounds took place in Germany (465), followed by France (312) and Spain (264). Although Sweden counted less active Venture Capital and Private Equity companies active in FinTech, it saw more funding rounds (214) than Ireland (150) and the Netherlands (136).

Half of the investment went into ten FinTech firms from Germany, Sweden, France, Ireland, Netherlands and Latvia.

*Figure 6: VC investment in FinTech, 2000-2020*




*Source: Technopolis analysis based on Crunchbase and Dealroom data*

In the EU27, the highest investments in FinTech went into firms such as Klarna. It is a Swedish eCommerce payment solutions platform for merchants and shoppers. Klarna has raised a total of €1.7 bn in funding over 22 rounds, the latest in October 2020 from a Corporate round. It is a regulated bank known for its 'buy now, pay later'

model that offers shoppers interest-free financing on retail purchases over a period of instalments.

Another example is N26 from Germany. N26 provides mobile banking services for its customers. The online banking service includes the handling of current accounts, fixed accounts and letting customers manage and control their banking details via a smartphone application easily. It has raised a total of €638 m in funding over 8 rounds. Its latest funding was raised in May 2020 from a Series D round. Its most recent investors include the Chinese Tencent Holdings and the New York based Valar Ventures.

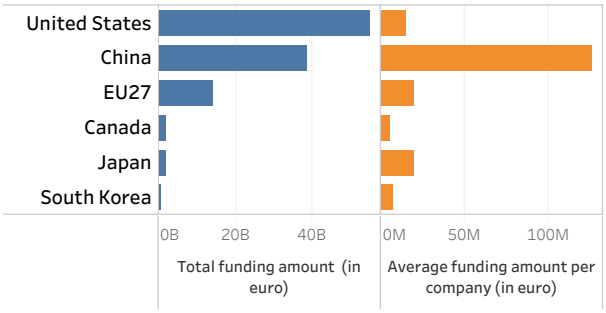
The top ten investments include the Latvian 4finance, a fast growing online and mobile consumer lending group with operations in 16 countries. Putting innovative data-driven analysis into all aspects of the business, 4finance has grown rapidly, issuing over €5 bn in single payment loans, instalment loans and lines of credit. 4finance operates through a portfolio of market leading brands with strong regional presence.

A similar recent analysis[46] on venture capital investment in the area of FinTech conducted by Finch Capital in 2020 concluded that European governments have provided a huge amount of support for FinTech startups in the most recent years. Nevertheless, startups and scaleups are expected to face a harsher market test for raising additional funding in the upcoming period. According to their findings, an issue for the EU is the lack of large ticket investors and mergers and acquisitions for FinTech startups. For scaleups below €0.5 bn, they expect a massive consolidation in the coming year with a focus on profitability to meet the needs of private equity firms.

Based on Crunchbase data, venture capital investment can be compared internationally, although the data have to be interpreted with caution (see Figure 6). US VC and private equity investments surpassed the €50 bn mark in the period 2015-2020. The analysis found that other global regions remain behind in terms of funding of FinTech in absolute terms, but China and the EU27 perform better when looking at the average funding amount per FinTech company.

The American figures are mostly driven by ten major investments that accounted for over a quarter of the funding amount in FinTech. These firms include SoFi, a finance company that offers a range of lending and wealth management services; Kabbage, a FinTech company that offers cash flow management solutions to small businesses; and Stripe, a developer-oriented commerce company helping small and large companies accept web and mobile payments. After China, the European Union witnesses the highest amount of funding, followed by Canada and Japan.

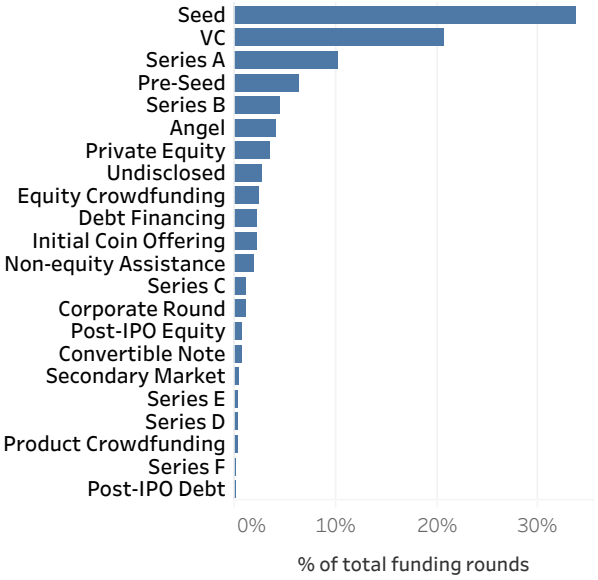
*Figure 7: Total VC and private equity funding in FinTech, in international comparison in € (in the period 2015-2019)*




*Source: Technopolis analysis based on Crunchbase and Dealroom data*

The figure below shows the prominence of different funding types in the FinTech industry within the EU27 countries from 2010 until 2019.

*Figure 8: Type of funding in the financial and banking sector (2010-2019)*




*Source: Technopolis analysis based on Crunchbase and Dealroom data*

The largest number of funding has been seed capital, which indicates that most funding was allocated to getting new business started in the first place. This is followed by VC and Series A funding, which helped to strengthen and further scale businesses.

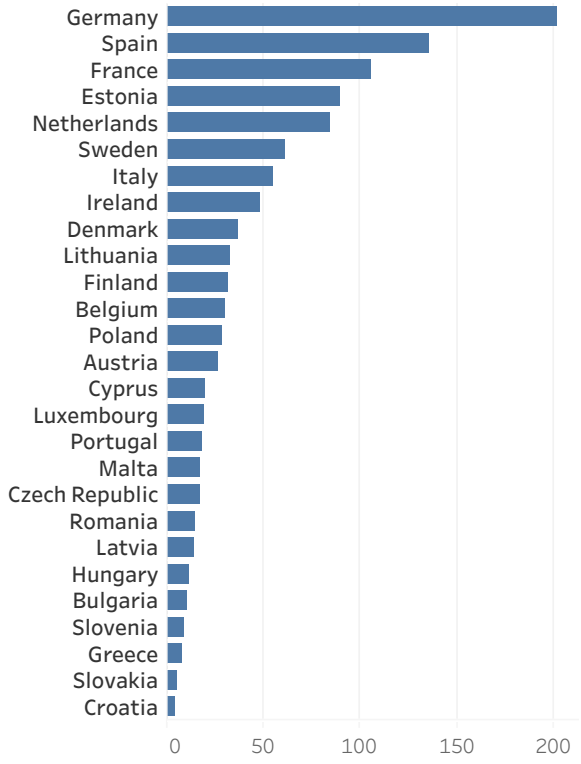
[46] https://www.finchcapital.com/post/state-of-european-FinTech-2020

## 3.2 Startup hubs in FinTech

The financial and banking sector is being transformed by FinTech startups that rewrite the rules of the world of finance. In total, there were 1 135 startups[47] active in FinTech in the EU27 in the period of 2015-2020 according to the merged dataset of Crunchbased and Dealroom.

The figure below presents the number of startups in the EU27 with countries boasting the highest number of startups on the top. In line with the venture capital and private equity figures, the highest concentration of startups in FinTech can be found in **Germany, Spain, France, but also Estonia** stands out.

*Figure 9: Number of startups in FinTech, by EU Member State (2015-2020)*



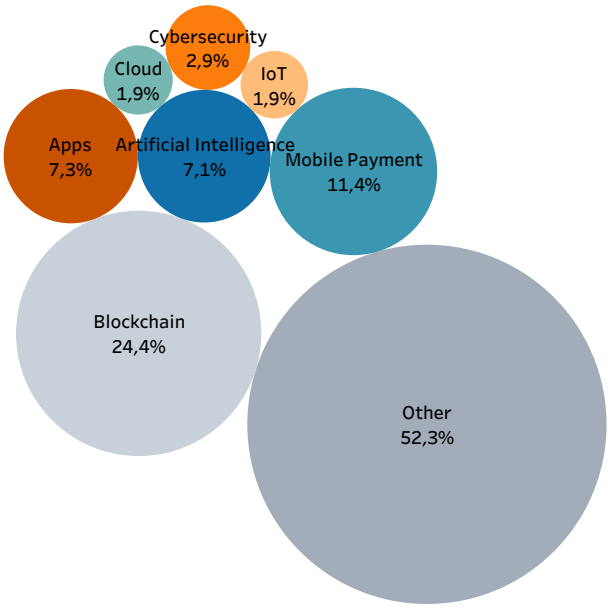

*Source: Technopolis analysis based on Crunchbase and Dealroom data*

Indeed, Estonia is often considered as a cashless society with over 99% of financial transactions occurring digitally[48]. Electronic ID and blockchain financial applications are quickly spreading. The analysis identified 89 Estonian FinTech startups established after 2015 that range from innovative startups such as TransferWise to blockchain leader Guardtime.

Most startups focus on financial software and internet solutions (more than 50% represented by the category 'Other' in Figure 9, since these are FinTech startups not linked to any highlighted technology field). **Blockchain, cryptocurrency, bitcoin represent the technological focus** of 24% of FinTech startups. Most of these blockchain startups are located in Estonia. For instance, Crypterium develops mobile apps that allow instant payments in cryptocurrency. Another Estonian startup called IronX is a joint venture between one of the global leaders in online trading, the IronFX Group and EmurgoHK, one of the global leaders in Blockchain technology. EmurgoHK created the decentralised public Blockchain Cardano[49] and the hugely successful ADA Coin. The objective of the joint venture is to create a fully regulated exchange ecosystem licenced from the Estonian Financial Intelligence Unit.

**Financial apps and mobile payment solutions** are also areas that have received high interest from startups. **Artificial Intelligence** (including machine learning) has been the topic of 7% of startups geographically concentrated in Germany, France, Italy and Spain.

*Figure 10: Type of FinTech startups, per category (2015-2020)*




*Source: Technopolis analysis based on Crunchbase and Dealroom data*

Compared to these specialisations, Cybersecurity falls somewhat behind, with only 33 startups founded in this area after 2015. Still, cybersecurity is more embedded in banking startups than the advanced technologies of cloud, robotic process automation and Internet of Things. The relatively low number of Cybersecurity startups may be explained by the substantial internal investments needed from banks. American banks like JPMorgan

[47] In this report FinTech startups are defined as companies that have been founded after 2015.

[48] https://www.crowdfundinsider.com/2020

[49] https://cardano.org/

Chase and HSBC each spend up to €600 m on cybersecurity annually.[50] International research from Lloyds Bank shows that 70% of senior decision-makers in the financial sector plan to invest in Cybersecurity within the next 12 months and 10% within 1-3 years.[51] For Cloud technology these numbers sit at 60% and 14%. In response to these internal Cybersecurity investments, startups may focus on other business niches.

[50] American Banker, 2019.

[51] Lloyds Bank, 2019.

Section 4

# 4. Skills supply and demand

**Key messages**

The demand is high for professionals with advanced technology skills within the financial services and banking sector. Within the registered professionals on LinkedIn and employed in financial services and banking, **Big Data** represents far way the highest share in the EU27, reflecting a particularly important role of this field of technology for this sector. Big Data is followed by **Cloud technologies, Artificial Intelligence, Cybersecurity, Internet of Things and Blockchain**. Emerging technological skills such as Artificial Intelligence and Internet of Things, both aimed at improving customer services, are rapidly gaining in importance.

The analysis of company reports in the sector shows that the top skills with the highest 1-year growth included several **programming skills** (Python, R, C, PHP) but also **analytical skills, client management** and **soft skills** such as **team spirit and creativity**.

In terms of the relative share of advanced technology professionals employed in the financial services and banking sector, we find that the Baltic states and Nordic countries rank on the top such as Estonia, Lithuania, Ireland, Finland but also Hungary and the Netherlands.

## 4.1 Availability of new technological skills

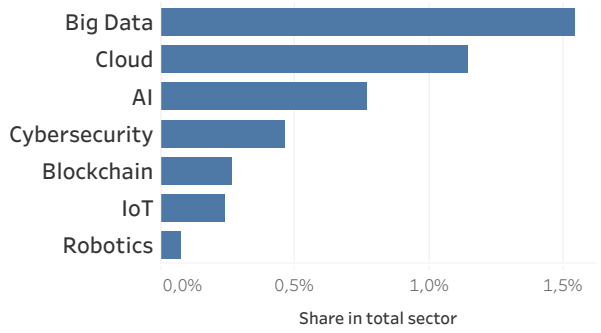
The financial services and banking sector is one of the early adopters of new technologies, therefore skilled professionals are in high demand. In general, they are expected to have experience both in the financial domain and in advanced technologies[52].

This report explored the supply and demand of technology professionals employed in the financial services and banking sector based on data from the self-reported skills of professionals in LinkedIn, a widely used and accepted online job platform. The database provides a unique opportunity to enrich our understanding of the supply of skills with a level of granularity that is not available in any of the traditional data sources. The number of skilled professionals employed across different economic sectors can also give some indication about the level of technology uptake in industry.

Figure 10 visualises the share of professionals with advanced technological skills employed in the financial and banking sector in 2020 based on the analysis of LinkedIn[53] data. Within the registered professionals, **Big Data** represents far way the highest share in the EU27, reflecting a particularly important role of this field of technology for this sector.

Big Data is followed by Cloud technologies, Artificial Intelligence and Cybersecurity. The financial services and banking sector also employs professionals with skills in Blockchain, Internet of Things and Robotics.

*Figure 11: Share of professionals with advanced technological skills in the financial services and banking sector, EU27, 2020*




*Source: Technopolis Group based on LinkedIn analysis*

Big Data expertise is closely related to the sectoral change driver 'Data & analytics' (see section 1.3), for product management and strategic planning, rather than disruptive technologies.

The presence of Cloud technology expertise can be clearly understood as a reflection of the focus on cloud-hosted mobile applications within the sector.

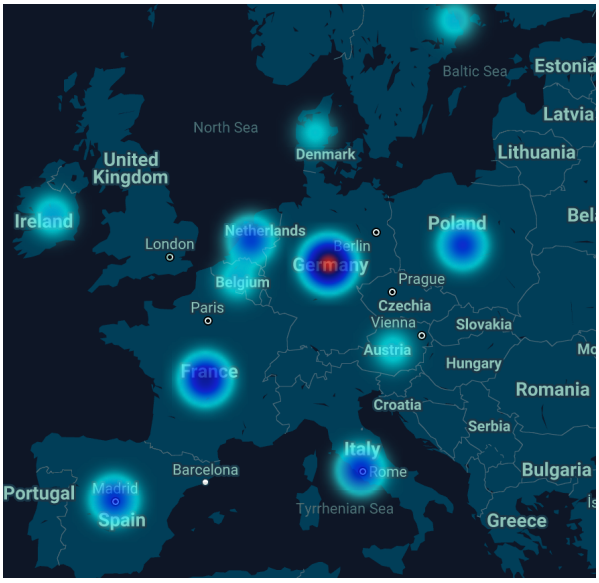
[52] Softest, 2020.

[53] To harvest the data from LinkedIn, keywords capturing skills by advanced technology have been defined and reviewed by technology experts. Queries have subsequently been constructed to filter the database by location and industry. To capture the financial services and banking sector the following categories have been used: financial services, banking, investment banking. In order to capture the number of professionals working in the sector, occupations related to financial services, banking have been taken into account. Please note that the total industry figure does not represent the full employment in the industry.

Blockchain technology skills play a significant role in financial innovations that are at the heart of this industry. Cybersecurity skills are key for the development of safe applications and services. Artificial Intelligence and machine learning knowledge can support developments in the areas of fraud detection, execute intelligent responses, market predictions and forecasts, and provide customer service and recommendations.

While Figure 11 illustrates the distribution of technological skills in the financial and banking sector across the EU27 countries that are above the median, Figure 12 displays all EU countries ranked by their share of advanced technology professionals employed in the financial services and banking sector within the total number of professionals in the sector.

*Figure 12: Concentration of professionals with advanced technology skills in the financial and banking sector in the EU27*



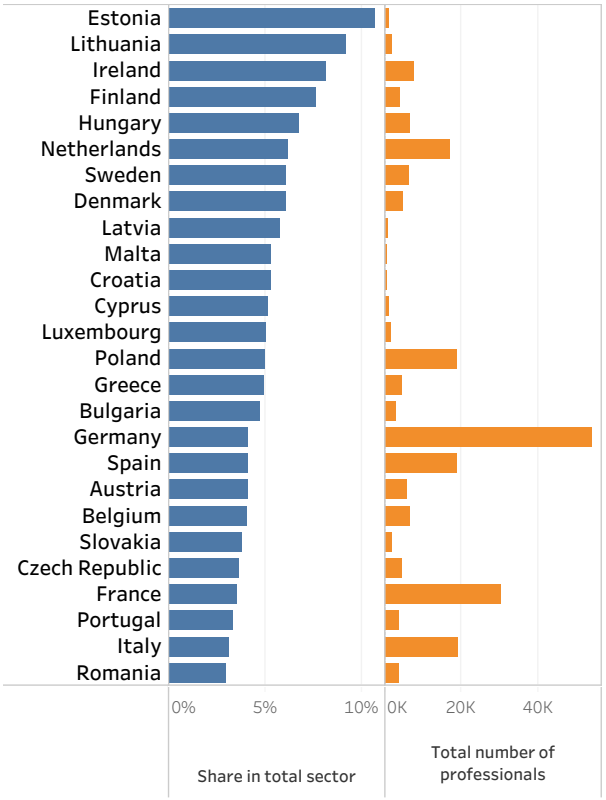

low high

*Source: Technopolis Group based on LinkedIn analysis*

It can be observed that in terms of the absolute number of advanced technology professionals employed in the sector, Germany, France and Italy stand out. When we look at the relative share of these professionals in the total sectoral professionals, we find that the Baltic states and Nordic countries rank on the top such as **Estonia, Lithuania, Ireland, Finland but also Hungary and the Netherlands**.

In Germany and France, the abundance of well-known specialists in the finance and banking industries form a solid foundation for the presence of FinTech skills.[54] This finding is further supported by the France FinTech Association.

*Figure 13: Share of AT skilled professionals within total sector on LinkedIn employed in the financial services and banking sector and total number of professionals corrected for representativeness, 2020*



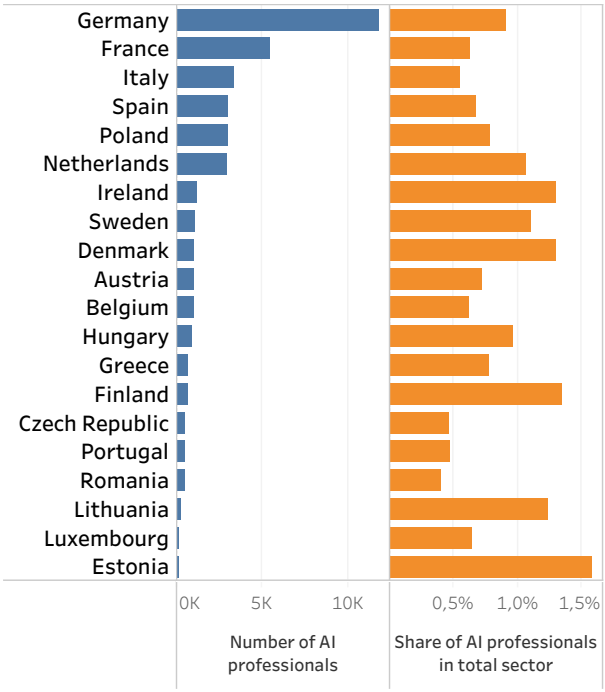

*Source: Technopolis Group analysis based on LinkedIn*

Note: Only countries with above median total industry professionals are displayed

Zooming in, Figure 13 demonstrates the allocation of the most represented technological skills' supply related to **Artificial Intelligence** across top performing EU countries. In terms of the relative shares within the total financial services and banking sector professionals, again Estonia is leading the list, followed by Finland, Denmark and Ireland. In terms of the absolute number of AI professionals employed in finance and banking and registered on LinkedIn, Germany, France and Italy are on the top of the country ranking.

[54] IT Europa, 2015.

*Figure 14: Financial services and banking sector professionals with Artificial Intelligence skills, 2020*



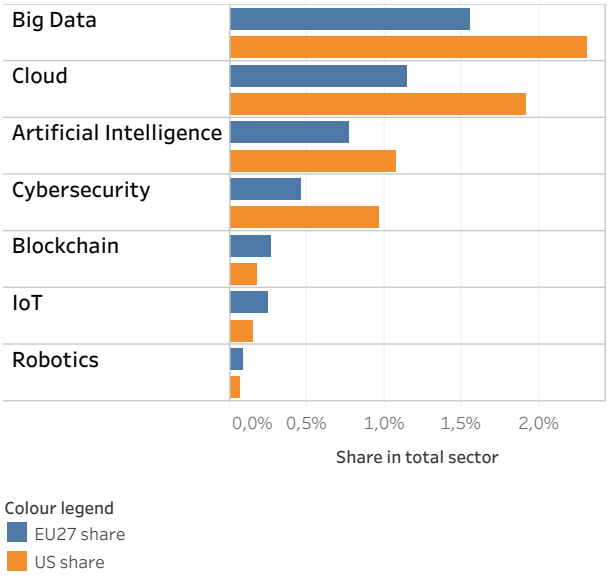

*Source: Technopolis Group based on LinkedIn analysis*

LinkedIn data also allow the comparison of the financial services and banking sector in terms of skilled professionals in the EU27 and the US. This is particularly interesting to compare, seeing the important role of the US in banking at global scale. After taking the share of professionals with advanced technology skills employed in the financial services and banking sector within the total number of professionals in the sector, it can be observed that the **EU27 has a lower share of professionals in most of the technological fields than the US** including Big Data, Artificial Intelligence, Cloud technologies and Cybersecurity as depicted in Figure 14. The EU27 is still trailing the Unites States and China in terms of Artificial Intelligence innovation and development.[55] The underlying reasons are the fragmentation of the EU's digital market, difficulties in attracting human capital and external investment, and the lack of commercial competitiveness.

The difference in the number of employees in Cybersecurity may be explained by the relative difference in cyber threats. For example, in the field of insurance, fraud was estimated to represent €13 bn in costs for Europe in 2017.[56] In comparison, conservative estimates claim that across all lines of insurance, fraud costs $80 bn (€65 bn) per year in the United States.[57]

Nevertheless, the EU27 has a higher share of professionals in Blockchain employed in the sector than the US.

*Figure 15: Financial services and banking sector professionals with skills in advanced technologies in the EU27 and US*



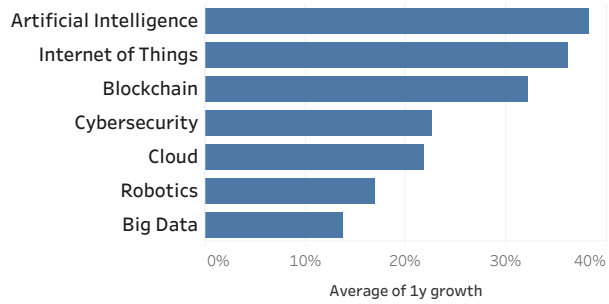

*Source: Technopolis Group based on LinkedIn analysis*

## 4.2 Demand for new skills

After analysing the availability of technological skills in the financial services and banking industry, it is also important to look at which skills have been the most common in the recent hires. To measure this demand, first, the 1-year growth rate of technological skills has been analysed by comparing the skills indicated in 2019 and its change to 2020.

Figure 15 visualises the advanced technological skills that showed the highest growth within the last year (from 2019 to 2020). We see **Artificial Intelligence on top followed up by IoT and Blockchain.** This result emphasises the growing importance of digital technologies and digital skills in the financial and banking sector.

*Figure 16: 1-year growth of top 5 skills*




*Source: Technopolis Group based on LinkedIn analysis*

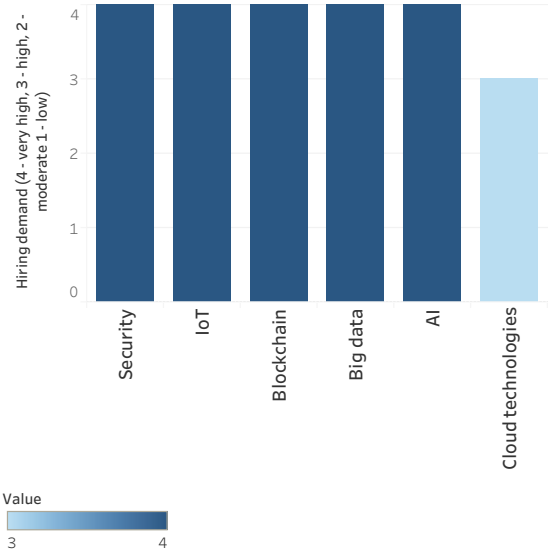
[55] Carnegie, 2020.
[56] Insurance Europe, 2018.
[57] Earlymetrics, 2020.

Emerging technological skills linked to **Artificial Intelligence** are becoming more critical as financial institutions adjusted to operating online. The LinkedIn data provides evidence for particularly high recent growth rates in these areas. The Internet of Things and Artificial Intelligence are both used for improvement of consumer experience.

Based on the skills requirements of the online job advertisements posted on LinkedIn by European banking sector firms, we observe that the fields with 'very high hiring demand' as captured in LinkedIn data and analysis include several of the advanced technologies relevant for the industry: **Artificial Intelligence, Cybersecurity, Internet of Things, Big Data and Blockchain**. Hiring demand is defined as the share of job ads published on LinkedIn and requiring specific skills (Figure 18).

In the times of the COVID-19 pandemic, financial institutions continued and even strengthened their digital transformation projects, which prompted more demand for technology specialists in the sector. The analysis of company reports in the sector shows that the top skills with the highest 1-year growth included several programming skills (Python, R, C, PHP) but also analytical skills, client management skills and soft skills such as team spirit and creativity (Figure 17).

*Figure 17: Hiring demand in the banking industry (Dec 2019 – June 2020)*




*Source: Technopolis Group based on LinkedIn analysis*

As other studies also confirm skills that are highly needed include[58]:

- Programming skills that are necessary to develop mobile applications, full-stack platforms and user-responsive websites
- Data science, which supports companies in risk evaluation and fraud prevention
- Test automation skills, which are instrumental in enhancing product features and speeding up the testing process.

*Figure 17: Top 50 skills with the highest 1-year growth in the financial services and banking sector in the EU27, 2020*


*Source: Technopolis Group analysis of LinkedIn data based on company reports*

[58] Softest, 2020.

Section 5

# 5. Future outlook: challenges and opportunities

## 5.1 Advanced technologies to show continuous growth

The global FinTech market is anticipated to **grow around 20% annually** (CAGR) in the period 2020-2025.[59] The market is expected to witness progressive growth and reach the market value of around €248 bn by 2025. The key reason for the growth of the FinTech market is the high investment in technology-based solutions by banks and firms. Moreover, the infrastructure-based technology and Application Programming Interfaces (APIs) are reshaping the future of the financial services industry, thus supporting the growth of the global FinTech market. Furthermore, financial technology companies are delivering low-cost personalised products enabled by the continuous development in the IT sector, leading to rising customer expectations, thereby, boosting market growth globally.

In Europe, **tech investments are expected to focus on solutions that improve operational efficiency** in the financial and banking sector. In a 2016 survey on FinTech, the majority of respondents considered the following segments to have the highest potential for the future of FinTech: 'investing and asset management' (55%), 'payments' (54%) and 'crowdfunding/lending' (52%).[60]

Together with legacy technology overhaul, the investment in improved operational efficiency is representing a **€20 bn cost saving**.[61] FinTech investments focusing on new customer offerings and pricing represent a total commercial value of up to €5 bn.[62]

## 5.2 The cybersecurity storm rages on

The growing number of cyber threats since the start of the COVID-19 pandemic has underlined the importance of Cybersecurity for the banking sector. The rapid development and implementation of new technologies is expected to cause **more sophisticated attacks**. The scale and severity of attacks has turned cybersecurity into a top priority both in the short term and long term.

Advanced technologies like Artificial Intelligence, help banks to resolve cybersecurity issues (e.g. via more precise fraud detection), but also pose new threats and risks to them (e.g. deep fakes). Three trends are particularly challenging. In the first place, more and more individuals, who are often not aware of the risks, will **access bank accounts via mobile devices** on which security standards may be lower. In the second place, **hackers increasingly target shared banking systems** and third-party networks to gain access to the bank infrastructure. To what extent will banking organisations be held responsible for their larger ecosystem is still to be seen. In the third place, cybercrime is invading **the growing world of cryptocurrency**. Especially when cryptocurrency becomes a commonly accepted type of payment, the intertwined systems of cryptocurrencies and other currencies may lead to new types of fraud.

Banking institutions play an important role in keeping our economy and society running. Timely and adequate communication and information sharing are expected to gain importance. Initiatives, such as the European FI-ISAC (European Financial Institutes – Information Sharing and Analysis Centre), show the **benefits of cooperation and help fighting cybercrime by promoting knowledge sharing and inter-organisational learning**. In the European Commission's public consultation on the Digital Operational Resilience Framework for Financial Services[63], specific input was gathered on threat and incident exchanges. This would help to strengthen information sharing among financial market participants, as well as more optimal cooperation among public authorities. Moreover, the largest financial infrastructures, Europol and the European Union Agency for Cybersecurity (ENISA) announced the Cyber Information and Intelligence Sharing Initiative (CIISI-EU)[64]. By joining forces, these entities seek to detect, prevent and respond to cyberattacks more holistically from this year onwards.

It is people that make the banking sector both safe as well as vulnerable. Cybersecurity incidents do not only stem from technical deficiencies and as long as the human factor plays a role in the cybersecurity field, investing in qualified staff and informing consumers about potential risks is

[59] PR Newswire, 2020.
[60] Roland Berger, 2016.
[61] Oliver Wyman, 2020.
[62] Oliver Wyman, 2020.

[63] https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf
[64] https://www.ecb.europa.eu/paym/intro/mip-online/2020/html/2009_mip_online.en.html

paramount. This means, **investing and strengthening the skillset of banking employees**, so that they are well-equipped to take advantage of advanced technologies (e.g. Artificial Intelligence) that lift cybersecurity levels. It is agility and flexibility that will make people and their organisations able to deal with ever enfolding threats. As the stakes are high, solid and reliable cybersecurity with well-trained employees may give banks a competitive advantage over those that faced large incidents or public scandals.

Although the banking sector with their payment services may be considered the primary segment with an interest in cybersecurity, other financial institutions will also feel a need to keep protecting the various data sets they manage, including financial transactions, geolocation and special categories of personal and other sensitive data. As such, it is expected they will follow the banks in their improvement of cybersecurity in the near future.

# Bibliography

Accenture, 2017. Mobile Banking Applications, https://www.accenture.com/t20180223T145013Z__w__/tr-en/_acnmedia/PDF-49/Accenture-Mobile-Banking-Apps-Security-Challenges-Banks.pdf

Accenture, 2019. Cost of cybercrime, https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

American Banker, 2019. Financial firms spend up to $3,000 per employee on cybersecurity, https://www.americanbanker.com/articles/financial-firms-spend-up-to-3-000-per-employee-on-cybersecurity

Asia Blockchain Review, 2019. https://www.asiaBlockchainreview.com/the-impact-of-Blockchain-on-banks-financial-institution/

Attila Security, 2019. Cyber Threats In The Banking Industry, https://www.attilasec.com/blog/banking-industry-cyber-threats

Bank Innovation, 2020. 2020's Top Cyber Threats in Banking, https://bankinnovation.net/allposts/resources/sponsored/2020s-top-cyber-threats-in-banking/#:~:text=Third%2Dparty%20Data%20Breaches%20and,and%20frequently%20backing%20up%20data

BitSight, 2019. Cybersecurity and Banking: 3 Trends to Watch in 2020, https://www.bitsight.com/blog/cybersecurity-and-banking-3-trends-to-watch-in-2020

Business insider, 2019. The impact of Artificial Intelligence in the banking sector & how AI is being used in 2020, , https://www.businessinsider.com/ai-in-banking-report

Capgemini, 2019. Reinventing cybersecurity with Artificial Intelligence, https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

Carnegy, 2020, Europe and AI: Leading, Lagging Behind, or Carving Its Own Way? https://carnegieendowment.org/2020/07/09/europe-and-ai-leading-lagging-behind-or-carving-its-own-way-pub-82236

China daily, 2020, Top 10 companies with most FinTech patent applications, https://www.chinadaily.com.cn/a/202008/11/WS5f31ccc0a31083481725f680.html

CIO.com/Economic Times, 2020. How this Dubai based bank fought phishing and DDOS attacks, https://cio.economictimes.indiatimes.com/news/digital-security/how-this-dubai-based-bank-fought-phishing-and-ddos-attacks/78009021

Cipher, 2018. FinTech – the importance of patents as banking and technology converge, https://cipher.ai/wp-content/uploads/2020/04/FinTech-report-understanding-the-role-of-patents.pdf

Cybercrime Magazine, 2017. Cybercrime Damages $6 Trillion By 2021, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

Deutsche Bank, 2016. Transaction Banking Cybersecurity Whitepaper, https://cib.db.com/docs_new/GTB_Cyber_Security_-_Whitepaper_(DB0457)_DIGITAL.PDF

Deutsche Bank, 2019. Artificial intelligence in banking, http://dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000495172/Artificial_intelligence_in_banking%3A_A_lever_for_pr.pdf

Dutch Ministry of Foreign Affairs, 2019. FinTech services in Europe, https://www.cbi.eu/market-information/outsourcing-itobpo/FinTech-services

Earlymetrics, 2020, Combatting insurance fraud with tech: a vicious cycle https://earlymetrics.com/combatting-insurance-fraud-with-tech-vicious-cycle/

EBF, 2020a. AI Paper, https://www.ebf.eu/wp-content/uploads/2020/03/EBF-AI-paper-_final-.pdf

EBF, 2020b. Cybersecurity, https://www.ebf.eu/priorities/cybersecurity-innovation/cybersecurity/

EBF, 2020c. Facts and Figures, https://www.ebf.eu/wp-content/uploads/2020/01/EBF-Facts-and-Figures-2019-Banking-in-Europe.pdf

ECB, 2020. Major European financial infrastructures join forces against cyber threats, https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200227_1~062992656b.en.html

ECSO, 2020. ECSO BAROMETER 2020: "CYBERSECURITY IN LIGHT OF COVID-19", https://www.ecs-org.eu/documents/uploads/report-on-the-ecso-members-and-the-community-survey.pdf

EIB institute, 2019. Mapping the FinTech Ecosystem in the EU, https://institute.eib.org/wp-content/uploads/2019/03/LSE_EIF_Capstone_2019_fv.pdf

ENISA, 2020. European Financial Institutes – Information Sharing and Analysis Centre, A Public-Private Partnership, https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership

ENISA, 2020. Understanding and dealing with phishing during the COVID-19 pandemic, https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic

Enterprise Ireland, 2019. The European Cybersecurity Market: Mapping the Opportunities and Route to Market for Irish SMEs, https://globalambition.ie/cybersecurity-report-and-conference/

European Commission, 2019. Consultation document – Digital Operational Resilience Framework for Financial Services, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf

European Economic and Social Committee, 2018. Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks – Study, https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/cybersecurity-ensuring-awareness-and-resilience-private-sector-across-europe-face-mounting-cyber-risks-study

European Payment Council, 2019. 2019 Payment Threats and Fraud Trends Report, https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2019-12/EPC302-19%20v1.0%202019%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf

European Systemic Risk Board, 2020. Systemic cyber risk, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

Europol, 2020. Enterprising criminals – Europe's fight against the global networks of financial and economic crime, https://www.europol.europa.eu/publications-documents/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime

Financial Times, 2018a. AI in banking: the reality behind the hype, https://www.ft.com/content/b497a134-2d21-11e8-a34a-7e7563b0b0f4.

Financial Times, 2018b. Tech giants leave banks in the dust in race for FinTech patents, https://www.fnlondon.com/articles/tech-giants-leave-banks-in-the-dust-in-race-for-FinTech-patents-20180802

Financial Times, 2020. Banks work with FinTechs to counter 'deepfake' fraud, https://www.ft.com/content/8a5fa5b2-6aac-41cf-aa52-5d0b90c41840

Finch Capital, 2020. The State of European FinTech 2020. https://www.finchcapital.com/post/state-of-european-FinTech-2020#:~:text=Finch%20Capital%20issued%20its%20annual,will%20shape%20FinTech%20in%202021.

Forbes, 2019, The 7 Biggest Technology Trends To Disrupt Banking & Financial Services In 2020. https://www.forbes.com/sites/bernardmarr/2019/11/08/the-7-biggest-technology-trends-to-disrupt-banking--financial-services-in-2020/

Gartner, 2020. Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020, https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem

IDC, 2020, Worldwide Big Data and Analytics Spending Guide. https://www.idc.com/getdoc.jsp?containerId=IDC_P33195

IMF, 2020, Financial Services: Getting the Goodsm https://www.imf.org/external/pubs/ft/fandd/basics/finserv.htm

ING, 2017, Katana gives bond traders a cutting edge, https://www.ing.com/Newsroom/News/Katana-gives-bond-traders-a-cutting-edge.htm

International Banker, 2020. Building a human firewall against cybercrime, https://internationalbanker.com/technology/building-a-human-firewall-against-cybercrime/

Insurance Europe, 2018, Insurance fraud: not a victimless crime https://www.laa.lv/wp-content/uploads/2020/01/Insurance-fraud-not-a-victimless-crime.pdf

Invyo, 2019. The European Top 50 of the most valued FinTech, https://insights.invyo.io/europe/mapping/the-european-top-50-of-the-most-valued-FinTech/

IT Europa, 2015. French financial technology group founded, https://www.iteuropa.com/?q=french-financial-technology-group-founded

Juniper, 2018. Robotic process automation revenues in banking & financial services to reach $1.2bn by 2023, https://www.juniperresearch.com/press/press-releases/Robotic-process-automation-revenues-in-banking

KPMG, 2018. Top 10 Drivers of Change in Banking, https://assets.kpmg/content/dam/kpmg/us/pdf/2018/09/top-10-drivers-of-change-banking.pdf

Lloyds Bank, 2019. Financial Institutions Sentiment Survey, https://resources.lloydsbank.com/insight/financial-institutions-sentiment-survey/

Minesoft, 2020. Understanding the FinTech Landscape, https://minesoft.com/2020/03/11/understanding-the-FinTech-landscape/

NVB, 2020. Digitaal met de mens centraal, https://www.nvb.nl/media/3360/nvb-visie-digitaal-met-de-mens-centraal.pdf

Oliver Wyman, 2020. Aim for revival. Not just survival. European Banking 2020 https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2020/jul/European-Banking-Outlook-2020.pdf

Positive technologies, 2018. Automated code analysis. web application vulnerabilities, https://www.ptsecurity.com/upload/corporate/ww-en/analytics/PT-AI-Statistics-2018-eng.pdf

PR Newswire, 2020, FinTech Industry Report 2020-2025 - Trends, Developments and Growth Deviations Arising from the COVID-19 Pandemic, https://www.prnewswire.com/news-releases/FinTech-industry-report-2020-2025---trends-developments-and-growth-deviations-arising-from-the-covid-19-pandemic-301080282.html

PwC, 2017, 'Artificial Intelligence and digital labor in financial services', https://www.pwc.com/us/en/industries/financial-services/research-institute/top-issues/artificial-intelligence.html

PwC, 2019. Global FinTech Report 2019, https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-FinTech-report-2019.pdf

PYMNTS.COM, 2020. ING, On The Use Of AI And ML In Financial Crime Prevention, https://www.pymnts.com/fraud-prevention/2020/ing-artificial-intelligence-machine-learning-fraud-prevention/

Roland Berger, FinTechs in Europe – Challenger and Partner, https://www.rolandberger.com/publications/publication_pdf/roland_berger_FinTech.pdf

Softest, 2020. In Demand Skills For FinTech Industry In 2020, https://softest.co/in-demand-skills-for-FinTech-industry/

Swift Institute, 2017. Forces shaping the cyber threat landscape for financial institutions, https://csis-website-prod.s3.amazonaws.com/s3fs-public/171006_Cyber_Threat_Landscape%20_Carter.pdf?UWqJEbDm.dBKSLEIFTyYs1IxJaExh9Y7

The Global Treasurer, 2019. The importance of cyber security in banking, https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-in-banking/

TNO, 2020. Shared Research Programma Cybersecurity, http://publications.tno.nl/publication/34636550/wByxS8/wolthuis-2020-shared.pdf

Verizon, 2020. 2020 Verizon Data Breach Investigations Report (DBIR), https://enterprise.verizon.com/resources/reports/dbir/

WTO, 2020. Developments in the sector, https://www.wto.org/english/tratop_e/serv_e/finance_e/finance_devel_e.htm

YS, 2019. How FinTech is revolutionising with Blockchain technology, https://yourstory.com/2019/10/FinTech-Blockchain-technology

# About the 'Advanced Technologies for Industry' project

The EU's industrial policy strategy promotes the creation of a competitive European industry. In order to properly support the implementation of policies and initiatives, a systematic monitoring of technological trends and reliable, up-to-date data on advanced technologies is needed. To this end, the *Advanced Technologies for Industry* (ATI) project has been set up. It provides policymakers, industry representatives and academia with:

- Statistical data on the production and use of advanced technologies including enabling conditions such as skills, investment or entrepreneurship;
- Analytical reports such as on technological trends, sectoral insights and products;
- Analyses of policy measures and policy tools related to the uptake of advanced technologies;
- Analysis of technological trends in competing economies such as in the US, China or Japan;
- Access to technology centres and innovation hubs across EU countries.

You may find more information about the 16 technologies here: https://ati.ec.europa.eu.

The project is undertaken on behalf of the European Commission, Directorate General for Internal Market, Industry, Entrepreneurship and SMEs and the European Innovation Council and SME Executive Agency (EISMEA) by IDC, Technopolis Group, Capgemini, Fraunhofer, IDEA Consult and NESTA.

*April 2021*

EA-08-21-010-EN-N

Publications Office
of the European Union