Lisbon School of Economics & Management
Universidade de Lisboa

MASTER

MANAGEMENT INFORMATION SYSTEMS

MASTER´S FINAL WORK

DISSERTATION

THE APPLICATIONS AND IMPLICATION OF EMERGENT TECHNOLOGIES IN THE FINANCIAL SECTOR

TIAGO ALEXANDRE TEIXEIRA BELLES ROSAS

JUNE - 2025

Lisbon School of Economics & Management
Universidade de Lisboa

MASTER

MANAGEMENT INFORMATION SYSTEMS

MASTER´S FINAL WORK

DISSERTATION

THE APPLICATIONS AND IMPLICATION OF EMERGENT TECHNOLOGIES IN THE FINANCIAL SECTOR

TIAGO ALEXANDRE TEIXEIRA BELLES ROSAS

SUPERVISION:

PROFESSOR ANTÓNIO PALMA DOS REIS

JUNE - 2025

In memory of José da Silva Belles Rosas,
Maria Indalécia Pereira da Rocha Teixeira, and
Matias Veloso Teixeira, who always supported me
and hoped I would achieve great thing

GLOSSARY

AI – Artificial Intelligence.

API – Application Programming Interface.

B2B – Business-to-Business.

CRM – Customer Relationship Management.

DDoS – Distributed Denial-of-Service.

DeFi – Decentralized Finance.

DLT – Distributed Ledger Technology.

DORA - Digital Operational Resilience Act.

EU – European Union.

GDPR – General Data Protection Regulation.

HFT – High Frequency Trading.

IoT – Internet of Things.

IMF – International Monetary Fund.

IT – Information Technology.

LSTM – Long Short-Term Memory.

MiCA – Markets in Crypto-Assets Regulation.

ML – Machine Learning.

OCR – Optical Character Recognition.

PSD2 – Second Payment Services Directive

PSD3 – Third Payment Services Directive

QML – Quantum Machine Learning.

RPA – Robotic Process Automation.

ABSTRACT

This study examines the evolving role of emergent technologies, including Artificial Intelligence, Machine Learning, Blockchain, Cloud Computing, IoT, and Quantum Computing, within the financial sector. As financial institutions adopt and integrate new technological innovations, they have been led to changes, such as Decentralized Finance, Algorithmic Trading, and Real-Time Regulatory Compliance. This research explores the applications, synergies, challenges, implications, and risks of these technologies as they alter more traditional financial operations. While most of the current applications are known and well documented, their future evolution still is unknown, therefore this study explores the possible implications of technology adoption, regulatory frameworks, and ethical considerations. Through a qualitative analysis integrating expert insights and secondary data, this study provides a perspective on the trajectory of these innovations and both the current and future possible impacts on the financial sector. Findings indicate that emerging technologies promise to improve operational efficiency, security, and customer service, while also enabling new financial models and greater inclusion. However, they also present some important challenges related to data privacy, cybersecurity, workforce adaptation, and regulatory compliance. This study highlights the necessity for proactive, flexible regulatory frameworks and continuous technological management so as to balance innovation with regulatory management. Ultimately, the successful evolution of financial technologies will depend on coordinated efforts between institutions, regulators, and stakeholders to bring opportunities while mitigating potential downsides.

KEYWORDS: Emerging Technologies; Financial Sector; Regulation; Technological Change.

JEL CODES: G20; G28; M15; O33.

Table of Contents

ACKNOWLEDGMENTS

First, I wish to thank Professor António Palma dos Reis for his encouragement and guidance.

I am very grateful to Mr. Luis Fernando de Carvalho, Mr. Pedro Magriço, and to all other people who wished to stay anonymous, for accepting doing the interviews, without them this work couldn't be completed.

Finally, I am thankful to my family, especially my parents, José Rosas and Elsa Rosas, and my grandmother, Maria da Conceição Rosas, for their patience and their support throughout the completion of this dissertation, as well as to my friends and colleagues who helped me along the way.

1. Introduction

The financial sector has continuously adopted the improvement of technology so as to enhance efficiency, security, engagement and relation with customers. In more recent years, once again, emerging technologies continue to change the way the financial sector operates, by optimizing traditional processes like fraud detection, risk management, and transaction processing, but also enabling transformative shifts, such as DeFi, algorithmic trading, and real-time regulatory compliance.

While current applications of these technologies are increasingly well-documented, the trajectory of their integration, especially in the short to medium term, remains mostly uncertain. This thesis tries to address that gap by combining expert insights with academic literature to explore both the present use and near-future potential of emerging technologies in the financial sector. Contributing to the understanding of how these technologies are likely to influence financial operations, regulatory dynamics, and strategic decision-making in the short to medium term. Therefore, the core research questions guiding this thesis are:

Question 1: Currently, what are the main emerging technologies being applied in the financial sector, where are they being applied, and what implications do they bring?

Question 2: How will emerging technologies influence the financial sector in the short and medium term?

Question 3: What are the potential regulatory challenges created by the expected evolution of emerging technologies in the financial sector?

This dissertation begins by explaining the methodology employed to gather and analyze data, detailing the approaches used to ensure the reliability and validity of the answers. This is followed by a review of existing literature on the financial sector, emerging technologies, and some regulation within the financial sector, providing a foundation for understanding the current environment and to later support or contradict the findings from the gathered results. The findings from the interviews are presented and then are subsequently discussed in relation to the current literature. Finally, the thesis concludes with a summary of the main contributions, reflections on the implications of the findings, and suggestions for future research directions.

2. Literature Review

2.1 Definition of the financial sector

According to the World Bank Group, the financial sector consists of institutions, instruments, markets, and legal and regulatory frameworks that help with transactions by granting credit. The development of the financial sector focuses on minimizing costs associated with acquiring information, enforcing contracts, and executing transactions. This process has led to the creation of financial contracts, markets, and intermediaries, shaped by varying combinations of costs and legal, regulatory, and tax systems across countries and historical periods.

The financial sector has five main functions: the creation of information regarding potential investments and allocation of capital; to oversee investments and to enforce corporate governance after the provision of finance; enable trading, diversification, and management of risk; mobilize and aggregate savings; and simplify the exchange of goods and services. (World Bank, n.d.-a)

2.2 Decomposition of the financial sector

Credit institutions

According to Banco de Portugal, credit institutions are comprised of banks, saving banks, mutual agricultural credit banks, central mutual agricultural credit banks, credit financial institutions, and mortgage credit institutions. (Banco de Portugal, n.d)

Banks are authorized to accept deposits or other repayable funds and engage in lending, including guarantees, financial leasing, and factoring. They offer payment services and trade in various financial instruments, including money market and foreign exchange instruments, financial futures, options, exchange and interest rate instruments, goods, and transferable securities. Banks also participate in securities issuance, provide advisory services on corporate strategy, and facilitate mergers and acquisitions. Additional activities include portfolio management, insurance mediation, credit reference services, safe custody services, and dealings in precious metals and stones. They may issue electronic currency, manage movable property leasing, and conduct other legal financial operations. Savings banks focus on accepting deposits and granting loans

secured by pledges or mortgages. They provide services such as cash transfers, rental of safes, real estate administration, and collection services. Additional operations are subject to authorization by the Central Bank. Mutual agricultural credit banks and the Central Mutual Agricultural Credit Bank accept deposits and offer agricultural credit to their members. Their services include safe custody, real estate management, insurance mediation, and credit referencing. They handle payments, securities placements excluding public subscriptions, and currency exchange. Other operations may be carried out with Central Bank approval. Credit financial institutions are permitted to engage in the same activities that banks are allowed to do, except the acceptance of deposits. Mortgage credit institutions specialize in granting, acquiring, and selling mortgage-backed credits on immovable property to issue mortgage bonds. They also manage credits involving central, regional, or local governments of European Union Member States, provided these are backed by legally binding guarantees, for the purpose of issuing public sector bonds. (Banco de Portugal, n.d.)

Financial Companies

Financial companies can be divided into investment firms and financial institutions with the exception of holding companies subject to the supervision of Central Banks. (Banco de Portugal, n.d.)

Investment firms can be categorized into dealers, brokers, wealth management companies, and foreign-exchange or money-market mediating companies. Dealers manage transactions involving financial instruments, including the receipt, transmission, and execution of orders on behalf of third parties. They oversee portfolio management, participate in public distribution offers, and provide investment consultancy. Their services extend to granting credit or securities loans for transactions, advising on capital structure and mergers, and assisting with public offerings of securities. Dealers also handle foreign exchange services and offer safe-deposit boxes tied to investment services. Brokers engage in similar activities, such as handling orders for financial instruments and managing third-party portfolios. However, their role in public offers excludes underwriting. They also provide securities registration, deposit services, and investment advice. Wealth management companies focus on managing third-party portfolios and offering specialized investment consultancy. Foreign-exchange or money-market

mediating companies facilitate money and foreign exchange market transactions while providing related services. (Banco de Portugal, n.d.)

Financial institutions include credit financial institution, financial leasing company, factoring company, mutual guarantee company, exchange offices, credit securitization, microcredit financial companies, real estate investment fund management companies, and securities investment fund management companies. Credit financial institutions conduct bank-like operations but do not accept deposits or provide payment services or electronic money issuance. Financial leasing companies specialize in leasing and may manage, or lease returned assets or other movable property. Factoring companies acquire short-term credits tied to the sale of goods or services in domestic and international markets. Mutual guarantee companies focus on financial operations and services to support small and medium-sized enterprises, micro-enterprises, students, and researchers. Regional development companies promote economic and social growth by funding investment projects and providing long-term credit to companies and independent professionals. Exchange offices handle foreign currency exchange, including purchasing gold, silver, and numismatic coins, while potentially acting as agents for payment or electronic money institutions. Credit securitization fund management companies facilitate the securitization of credit by acquiring, managing, and issuing securitized debentures to pay acquired credits. Microcredit financial companies extend small-value loans to individuals and entities initiating economic activities and offer advice and project monitoring. Real estate investment fund management companies manage real estate investment funds, provide consultancy for real estate investments, and handle real estate asset management on behalf of others. Securities investment fund management companies oversee collective investment schemes as per the legal framework, ensuring adherence to regulatory guidelines for portfolio management and fund operations. (Banco de Portugal, n.d.)

Payment institutions

Payment institutions are authorized entities responsible for providing and executing payment services. These services include enabling the placement and withdrawal of cash from payment accounts, along with all necessary operations to manage such accounts; facilitating the execution of payment transactions, such as fund transfers, direct debits, and transactions carried out using payment cards or similar devices; issuing and acquiring

payment instruments; conducting money remittance services; and executing payment transactions initiated via telecommunication, digital, or IT devices. (Banco de Portugal, n.d.)

Electronic money institutions

Electronic money institutions are legal entities authorized to issue electronic money. In addition to issuing electronic money, these institutions are allowed to provide payment services and grant credit related to specific payment services. They are also allowed to offer operational services and related ancillary services, such as providing guarantees for payment transactions, foreign exchange services, and services concerning the safekeeping, storage, and processing of data. These institutions may operate payment systems and engage in professional activities beyond the issuance of electronic money, in compliance with the applicable requirements for such activities. (Banco de Portugal, n.d.)

Insurance firms

According to the European Central Bank, insurance firms are financial intermediaries which provide direct insurance or reinsurance services, contributing to financial protection against risks and threats. Under an insurance policy, insurance firms agree to compensate policyholders for losses caused by predefined events in exchange for a fee or a premium. These firms have the role of facilitating savings by investing the collected premiums and allow risk pooling by distributing the losses among the policyholders. (European Central Bank, n.d.; Zee, 2004)

Insurance companies can be categorized into three main types: life insurance, general insurance, and reinsurance. Life insurance deals with risks related to an individual's life, providing services such as life insurance, whole life insurance, and annuities. General insurance deals with all risks except risks related to life. Reinsurance is a transaction between two insurers in which one insurer purchases coverage from another to share or transfer part or all the risks it does not want to retain in full. (Zee, 2004)

Insurers that provide life and/or general insurance generally fall into one of two categories, mutual insurers or proprietary insurers. Mutual insurers are owned by policyholders, who are the bearers of savings and residual risks. Meanwhile proprietary

insurers are owned by shareholders, in this case the owners bear the residual risks and sometimes the saving risks, and the policyholders may bear the saving risks. These companies are subject to strict regulations designed to ensure their solvency and protect the interests of their policyholders. (Zee, 2004)

Capital Markets

Capital markets are financial markets that facilitate the trading of financial assets such as stocks, bonds, and other securities. They allow businesses to raise long-term funds by offering market securities through both debt and equity. This allows companies to secure the financial capital necessary for growth, innovation, and job creation. Through capital markets, businesses can sell stocks, offering partial ownership to investors, or issue bonds, which are loans that must be repaid with interest. These markets are important for reducing the costs and risks associated with raising capital, thereby strengthening the economy by providing businesses with efficient access to funding. (International Finance Corporation, n.d.; Federal Reserve Bank of St. Louis, 2017)

Nonbanking Financial Institutions

A non-banking financial institution is a financial entity that does not hold a full banking license and cannot accept deposits from the public. These institutions provide financial services that banks do not typically offer, including investment services, financial consulting, brokering, money transmission, and check cashing. Non-banking financial institutions provide an alternative source of consumer credit, operating alongside licensed banks. Some examples of nonbanking financial institutions include insurance companies, contractual savings institutions, venture capitalists, market makers, specialized sectoral financiers, currency exchanges, microloan organizations, and pawn shops. (World Bank, n.d.-b)

While nonbanking financial institutions complement banks by offering alternative financial services, they also introduce competition and can specialize in particular sectors. However, in countries with weak regulatory frameworks, nonbanking financial institutions, particularly those within the shadow banking system, can create threats to the financial stability by operating with less management. (World Bank, n.d.-b)

Financial Regulatory Authorities

A Financial Regulatory Authority is an entity responsible for supervising and enforcing the rules and laws that govern financial institutions and markets. These institutions, such as banks, insurance companies, and asset managers, must adhere to these regulations to ensure stability and protect consumers. The role of such authorities extends beyond rule-setting; they are also responsible for ongoing supervision to ensure compliance. Financial regulatory authorities can also take enforcement actions when firms fail to comply with the rules, including issuing fines or initiating proceedings. Furthermore, they play an important role in managing financial institutions' resolution, which involves minimizing harm to the economy when a financial institution faces failure. (Central Bank of Ireland, n.d.-a)

Fintech

FinTech refers to the use of technology to deliver financial services and products to consumers. It includes a variety of areas within finance, including banking, insurance, and investing. FinTech allows consumers to access financial services more easily and quickly, often via the internet. FinTech products tend to be more accessible, providing consumers with a greater choice of services and products, since FinTech companies may not rely on traditional infrastructures like branch networks, they can offer more competitive prices. Technology also allows these companies to collect and store vast amounts of data, helping to create personalized services for consumers. However, the appearance of new business models in FinTech might lead to some challenges, as consumers may find it difficult to assess which companies are regulated and understand their rights if issues arise. Additionally, while FinTech increases accessibility for many, it could exclude those who are not familiar with digital tools, such as the internet or mobile devices, leaving them at a disadvantage. (Central Bank of Ireland, n.d.-b)

Ancillary Services

According to the EU law, financial ancillary services can be described as activities that are closely related to the core functions of banking but are not the primary banking

activities themselves. These services can be provided either to other entities within a corporate group or to external clients. Some of the most common ancillary services include operational leasing, the management or ownership of property, and the provision of data processing services. Additionally, the European Banking Authority may identify other activities that are similar to those listed and classify them as ancillary services to banking. (EUR-Lex, 2024)

2.3 Emerging technologies

To help better understand the subject, this thesis initially focuses mostly on six emerging technologies: Artificial Intelligence, Machine Learning, Internet of Things, Blockchain, Quantum Computing, and Cloud Computing. These technologies were selected due to their frequent mention in peer-reviewed articles and due to their recognition in the financial sector as some of the most influential and/or widely implemented technologies within the financial sector (Thompsett, 2025; Beau, 2024). While many technologies are impacting finance, these six stand out because of their versatility across various applications, their scalability, and their significant potential to transform the industry. Scientific reports consistently highlight these technologies as some of the main factors of financial innovation. Additionally, experts often identify AI, Quantum Computing, and Cloud Computing as foundational technologies expected to redefine fintech business models in the coming years (Marr, 2024; Fong et al., 2021). Collectively, these technologies support a broad spectrum of financial advancements. AI and ML enable sophisticated data analytics, the Internet of Things facilitates real-time connectivity, Cloud Computing provides flexible and scalable infrastructure, Blockchain ensures improved transparency and security, and Quantum Computing promises to deliver more powerful computational power (Beau, 2024; Fong et al., 2021).

After the initial analysis, additional technologies were included in the literature review based on patterns that emerged from the results. These included Neurocomputing, APIs, and RPA, which were not part of the original focus but became relevant due to their recurring presence and potential impact shown in the data.

2.3.1 Artificial Intelligence

According to Deloitte, artificial intelligence can be described as the capability of computer systems to perform tasks that would usually require human intelligence. These systems should be able to reproduce tasks that may include but are not limited to visual perception, speech recognition, pattern recognition, prediction, recommendation, learning, and/or language translation. However, it is important to highlight that the set of tasks considered to require human intelligence will evolve over time as new technologies are developed and adopted (Schatsky, Muraskin & Gurumurthy, 2014).

AI algorithms are increasingly being utilized for fraud detection in the financial sector. These systems analyze vast volumes of transactional data in real-time to identify irregular patterns and potentially fraudulent activities. With ML techniques, AI systems can continuously learn from new data, improving their ability to detect and prevent fraud more effectively over time (Jain, 2023; Manikandan et al., 2024).

AI became essential in assessing the credit score of individuals and businesses. By utilizing ML, these models analyze a wide range of variables and data, leading to the creation of more accurate and fair assessments of risk. Unlike traditional methods, AI considers broader parameters, including behavioral and contextual data, enabling financial institutions to make better-informed lending decisions and expand access to credit (Jain, 2023; Manikandan et al., 2024).

It is also being applied in AI-powered virtual assistants, such as chatbots, which have transformed customer service and experience in the financial sector. These systems provide personalized and efficient support to customers by addressing queries, resolving issues, and offering recommendations. With 24/7 service and the ability to handle multiple interactions simultaneously, AI customer service tools improve the overall customer experience by reducing wait times and lowering operational costs (Jain, 2023; Manikandan et al., 2024).

Investment management is another area where AI is making a good impact. By analyzing great amounts of data, news, and historical patterns, AI systems are used for portfolio management, risk assessment, and developing trading strategies. Its ability to process real-time data and predict trends has improved investment performance and risk mitigation, making it a formidable tool for financial institutions and individual investors (Manikandan et al., 2024).

The adoption of AI in menial tasks has resulted in significant cost savings. Automating tasks reduces the need for extensive human intervention, lowering general costs. AI also enhances risk management, minimizing the likelihood of financial losses. These cost efficiencies enable financial institutions to offer competitive pricing and allows them a better allocation of resources (Jain, 2023; Manikandan et al., 2024).

While AI offers immense benefits, it also presents challenges that must be addressed. One major concern is data privacy and security. Financial institutions handle large volumes of sensitive customer data, necessitating robust security measures to prevent breaches and comply with data protection regulations. Encryption, secure storage, and compliance with privacy laws are critical to safeguarding customer information (Manikandan et al., 2024).

Other challenges that AI brings are ethical challenges. AI can inadvertently perpetuate biases present in data, leading to discriminatory outcomes. As such, regular monitoring, evaluation, and adjustment of AI models are essential to ensure fairness and avoid biased results. Also, financial institutions must ensure transparency in AI decisions and accountability for automated outcomes. Establishing ethical frameworks and guidelines is necessary to manage the responsible development and deployment of AI (Manikandan et al., 2024).

As such, the EU has created the AI act which applies a risk-based framework that categorizes AI applications into different risk levels. Currently the AI act has determined that the applications to be considered as high-risk applications are the ones considered to significantly impact people's rights and safety, in the financial sector some of the better-known cases are in but not limited to credit scoring, loan approval, fraud detection, insurance claims processing, algorithmic trading and market analysis, and others (European Union, n.d.).

Still, AI's potential is far from over. Innovations, such as improved ML models and the appearance of quantum computing, brings new possibilities, from enhanced predictive analytics to faster, more secure transaction processing. However, these advancements will also introduce new complexities, particularly in data privacy and regulatory oversight. To be able to accompany the evolution of AI financial institutions must adopt flexible strategies, that ensure responsible AI integration that maximizes benefits while minimizing risks (Manikandan et al., 2024; European Union, n.d.).

Expected Evolution

AI adoption has become widespread across industries, with approximately 90% of institutions integrating AI technologies and planning to increase investments. Despite this, many organizations remain in early stages of implementation and lack substantial generative AI expertise. Nevertheless, 72% of executives intend to boost AI-related spending, and 69% expect AI to significantly enhance productivity (Moscetti & Bali, 2025).

Within the financial sector, institutions prioritize AI applications that optimize internal operations, enhance customer service, and combat financial crime, which are areas anticipated to deliver the most significant benefits over the next three years. Generative AI, especially large language models delivered via cloud platforms, are the main reasons for this growth. These technologies improve operational efficiency by automating tasks such as code generation and information retrieval. Additionally, AI-powered analytics help firms better understand customer preferences, such as predicting preferred payment methods, thereby improving customer interactions (Bank of England, 2025).

In financial services, AI use is expanding beyond process optimization into specialized domains. Lenders are utilizing AI to incorporate diverse data sources, increasing credit access for small and medium-sized enterprises, and promoting financial inclusion. Credit risk management, though nascent in AI adoption, increasingly employs techniques such as gradient boosting decision trees for pre-screening and pricing decisions. Insurance companies widely use AI models for underwriting and pricing, and emerging technologies like telematics facilitate personalized insurance products and enhanced risk management (Bank of England, 2025).

Financial markets are also using AI to optimize trading strategies. While fully autonomous AI trading systems remain uncommon, ongoing innovation points toward their future adoption. Investment managers utilize generative AI to analyze alternative data sources, including social media trends, to gain insights that enhance investment strategies and market efficiency (Bank of England, 2025).

Looking forward, long-term projections suggest generative AI could boost productivity in banking, insurance, and capital markets by up to 30% over the next 15

years. Public sector entities similarly recognize AI's potential to improve operational effectiveness. However, despite these promising opportunities, AI also presents systemic risks that require careful regulatory oversight to ensure financial stability (Bank of England, 2025; Leitner et al., 2024).

Expected Challenges

AI adoption in the financial sector faces multiple challenges spanning workforce readiness, regulatory uncertainty, and technological limitations. Many institutions report gaps in AI expertise and feel they lag behind peers, particularly in the banking sector and in the wealth management sectors, which indicates uneven progress across the industry (Moscetti & Bali, 2025).

Consumer skepticism can also further complicate AI adoption. A significant portion of customers either perceive AI tools and services as security risks or completely avoid them, creating a trust deficit that banks must overcome. Internally, challenges such as data privacy concerns, regulatory compliance, and cybersecurity risk are still some of the principal barriers to a broader adoption of this technology (PYMNTS, 2024).

Additionally, risks related to algorithmic bias, hallucinations, and potential misuse may distort financial market outcomes and undermine operational frameworks. These issues can systematically bias information processing, affecting institutions' risk management and decision-making capabilities, leading to more complexity in AI implementation within the financial sector (Bank of England, 2025; Leitner et al., 2024).

Correlation of Data Quality and Artificial Intelligence

The effectiveness and reliability of AI and ML depend on the quality of data. Poor data quality, such as noisy or missing labels, directly undermines model generalization and leads to inaccurate predictions on unseen data. This is especially important in supervised learning, where corrupted or incompleted labels can distort the training process and impair model performance. However, many current approaches for handling noisy data remain insufficient, as they either accumulate noise during training or only utilize a fraction of the available data, limiting the models' capabilities (Whang et al., 2023).

In the broader context of deep learning, the emergence of data-centric AI focuses on the increasing necessity of prioritizing data quality over model complexity. Key areas such as data collection, cleaning, validation, and integration, when combined with robust and fair model training, are essential for achieving dependable AI systems (Whang et al., 2023).

Expected Evolution of Workforces

As AI evolves, the market demands both new AI-specific skills and broader adaptability. While roles directly focused on AI development, such as data scientists and AI specialists, are growing, these professionals remain a minority in the workforce. Most employees will interact with AI as a tool embedded in their workflows, requiring new skills in collaboration, interpretation, and decision-making alongside AI systems, even without deep technical expertise (Green, 2024).

To be able to follow this evolution in technology, proactive investment in AI education and on-the-job training is essential. Embracing AI-related learning opportunities positions workers and organizations to innovate and adapt in a technology-driven market. Leaders are encouraged to replace fear of job displacement with strategic upskilling initiatives that empower employees and utilize AI as a productivity-enhancing and transformative force (Mayer et al., 2025).

A framework developed for incorporating a human supervisor within black-box AI models demonstrated significant improvements in performance and safety by enabling human intervention in uncertain or high-risk situations. This approach reduced the top-5 error rate by 5.2 percentage points, demonstrating that integrating human management can significantly improve AI system accuracy by enabling correction of errors that the AI alone might overlook. Moreover, human supervision is capable of enhancing operational safety by effectively identifying challenging situations where AI performance may degrade, allowing the prevention of adverse outcomes (Fridman et al., 2017).

2.3.2 Machine Learning

Fraud detection has been one of the most important roles of ML in the financial sector. The usage of algorithms such as Random Forest or LSTM have shown exceptional

accuracy in identifying fraudulent transactions. By analyzing documented data, ML can detect patterns and unusual behavior, flagging them for further investigation. However, issues like computational complexity and biased datasets become adversities for large-scale implementation (Ekiye & Hewage, 2024; Narayana & Panigrahi, 2024).

Another clear application of ML is in risk management. ML algorithms analyze historical data to identify patterns and predict future trends, which becomes a relevant part in mitigating credit, market, and operational risks. For instance, financial institutions tend to use ML to predict stock prices, interest rates, and market volatility, allowing them to make the most optimal decisions. Some companies have successfully integrated ML into their credit risk models, achieving significant improvements in predictive accuracy. The scalability of ML allows organizations to monitor and manage risks across diverse portfolios (Agrawal et al., 2024; Kour, 2024).

ML has further developed trading and investment strategies by enabling real-time analysis of market data. Automated trading systems consider the information gathered from this analysis to execute transactions based on predefined rules, leading to an increase in efficiency and a reduction on human bias (Agrawal et al., 2024; Kour, 2024).

The insurance industry is currently utilizing ML to predict claims and detect fraudulent activities with higher accuracy. ML models have shown better capabilities in analyzing claims data, leading to the reduction of losses and optimization of operations (Ekiye & Hewage, 2024; Narayana & Panigrahi, 2024).

Through personalization and improved customer service ML is currently being applied in customer service, leading to an enhancement in customer experience. By analyzing customer patterns, ML algorithms provide tailored financial recommendations and other suggestions. Natural language processing has also enabled the development of chatbots and virtual assistants for real-time support, which lead to the reduction of operational costs (Agrawal et al., 2024; Kour, 2024).

As more traditional models start to become obsolete due to their reliance in more limited variables such as income and credit history, ML model's role in credit scoring increased due to its capability to analyze diverse datasets, including alternative sources like social media activity. This more comprehensive analysis improves the accuracy of credit risk assessment and allows better loan decisions (Ekiye & Hewage, 2024; Kour, 2024).

Despite the capabilities of ML in the financial sector, its application still brings some consequences and challenges. Real-time systems require scalable designs to efficiently handle massive datasets. Deep learning boosts performance but demands heavy computation and often lacks transparency. Privacy issues and the lack of standardized datasets also lead to slower global adoptions (Narayana & Panigrahi, 2024; Kour, 2024).

2.3.3 Blockchain

Blockchain synchronizes stored data among peers on all computers or servers participating in a network. This creates multiple identical records, where all nodes in the network validate, verify, and agree on any changes or additions. Blockchain can be used for record keeping, transferring value, and smart contracts, which automatically execute transactions when predefined conditions are met. Once data is stored on the blockchain, it cannot be manipulated or changed, this is due to the fact that each block is connected to each other. This means that the timing, the order, and the content of the transactions cannot be altered, and blocks cannot be replaced unless all nodes agree with the proposed changes (Deloitte, 2018-a).

Blockchain's distributed ledger technology makes sure that transactions are recorded in a secure and immutable form, leading to the reduction of the possibility of fraud and unauthorized alterations. By providing transparent audit trails, blockchain increases trust among stakeholders and simplifies regulation compliance. However, while blockchain might be one of the most secure systems, it is still vulnerable to 51% attacks, smart contract exploits, problems with private key management, sybil attacks, and others (Deloitte, 2018-a; Sarda et al., 2018).

DeFi platforms allow blockchain to offer peer-to-peer transactions without the need for any intermediaries. Another benefit is that blockchain allows the creation of smart contracts, which are self-executing contracts which allow for the automation of transactions when predefined conditions or rules are met. On the contrary, more traditional payment systems don't have access to smart contracts and usually have higher costs and bigger delays due to the involvement of multiple intermediaries and more complex regulatory frameworks. Which might lead to a potential disruption in more traditional banking models (Panduro-Ramirez et al., 2022; Vukovljak, 2023).

While decentralized systems can bring some benefits, they can also bring problems in enforcing regulations, in monitoring transactions, and in preventing illicit activities. As such, there is a need to develop frameworks that can ensure that blockchain systems operate within legal and ethical boundaries (Deloitte, 2018-a; Yahiya et al., 2023).

Expected Evolution

The evolution of blockchain technology in the FinTech sector is propelled by multiple factors, primarily the rising demand for faster, cost-effective financial services that can operate seamlessly on a global scale. Advances in blockchain scalability and interoperability have significantly enhanced the efficiency of its applications, leading to increased investment and experimentation within the industry. Additionally, changing consumer behavior has contributed to the growing adoption of blockchain-based solutions, especially among digital natives seeking transparency, security, and efficiency in managing money and transactions (Globe Newswire, 2025).

Moreover, the growing shift toward digital currencies alongside heightened interest from traditional financial institutions further stimulates blockchain market growth. These factors, coupled with continuous technological innovations and evolving regulatory landscapes, are critical catalysts ensuring the robust expansion and dynamic development of blockchain applications in FinTech (Globe Newswire, 2025).

Financial Inclusion

Blockchain technology holds significant potential to enhance financial inclusion by bridging gaps left by traditional financial services and enabling broader access to the digital economy. One of the primary contributions of blockchain to inclusion is cost reduction, which directly addresses affordability, which is a major barrier for financially underserved populations (PricewaterhouseCoopers, n.d.).

Beyond affordability, blockchain enables the creation of innovative, locally tailored financial solutions that respond to specific inclusion challenges. Additionally, blockchain is able to reduce intermediaries and streamlines processes, allowing to increase the speed of payments. Interoperability is another crucial benefit, as protocols establish universal transaction rules, allowing integration across platforms and assets, which removes

barriers for both individuals and businesses accessing diferent types of services (PricewaterhouseCoopers, n.d.).

Advanced cryptography and secure consensus mechanisms inherent in public blockchain networks can ensure data integrity and make unauthorized tampering nearly impossible. This built-in security by design helps overcome mistrust in financial institutions and supports safer participation in digital financial ecosystems (PricewaterhouseCoopers, n.d.).

Privacy Concerns

Blockchain technology, while offering transparency and security, also presents significant privacy issues depending on its implementation. One major concern is the potential traceability of transactions linked to a specific entity, especially when a public key coincides directly with an individual's identity within the blockchain system. This situation is particularly worrying in public blockchains, where all participants can view transaction data, however it can still pose issues in private blockchains (Haro-Olmo, Varela-Vaca & Álvarez-Bermejo, 2020).

Selective disclosure mechanisms based on zero-knowledge cryptography have been proposed to address privacy concerns by allowing verification without exposing sensitive data. However, regulatory requirements such as the GDPR's "right to be forgotten" pose challenges for blockchain applications, especially in sectors where immutable records conflict with data deletion mandates (Haro-Olmo, Varela-Vaca & Álvarez-Bermejo, 2020).

Other possible issues include the costs associated with verifying data, auditing transactions, and ensuring interoperability among network participants. Pseudonymity in blockchain does not guarantee full privacy, as transaction analysis can potentially reveal users' identity by correlating incoming and outgoing transactions. Additionally, malicious actors within blockchain networks, particularly in IoT contexts, may threaten system integrity by masquerading as legitimate devices, complicating device identification and trust (Haro-Olmo, Varela-Vaca & Álvarez-Bermejo, 2020).

Moreover, distributed blockchain architectures introduce unique security challenges, including the high computational costs associated with consensus mechanisms.

Centralized alternatives exist but often reflect mutual distrust among participants due to fears of data manipulation. The absence of standardized protocols inhibits scalability and effective integration of blockchain with IoT systems. Crucially, the entire system's security hinges on the protection of private keys, emphasizing the need for robust key management to prevent unauthorized access (Haro-Olmo, Varela-Vaca & Álvarez-Bermejo, 2020).

2.3.4 Cloud Computing

Cloud computing is the delivery of computing services like software, storage, and processing power over the internet, allowing users to access and use applications without the need of infrastructures (Deloitte, 2018-b).

Cloud computing provides banks and financial institutions with an increase in efficiency, security, scalability, and cost reduction. By utilizing cloud computing, financial organizations can optimize operations and enhance customer experiences, gaining a competitive advantage. However, despite its numerous advantages, cloud adoption can also bring some challenges related to security, regulatory compliance, and management (Misra & Doneria, 2018).

Security is a great concern in the financial sector, where sensitive customer data must be protected from breaches and cyber threats. Cloud computing addresses these concerns by offering robust security features such as encryption, multi-factor authentication, and access controls. Cloud service providers implement advanced security protocols to safeguard financial data, reducing the risk of cyberattacks and unauthorized access. Moreover, cloud platforms enable real-time monitoring and threat detection, ensuring proactive security management (Misra & Doneria, 2018; Vadisetty, 2024).

Cloud computing allows financial institutions to scale their computing resources up or down based on demand. This flexibility is beneficial during peak transaction periods, ensuring seamless operations without the need for costly on-premises infrastructure. By adopting cloud solutions, banks can quickly adapt to market changes, deploy new financial products, and enhance service delivery with minimal delays (Vadisetty, 2024).

Traditional IT infrastructure requires significant capital investment in hardware, software, and maintenance. Cloud computing eliminates these expenses by offering a pay-

as-you-go model, allowing financial organizations to pay only for the resources they use. This cost-effective approach enables banks to allocate funds toward innovation, customer experience improvements, and business expansion, rather than IT maintenance. Additionally, cloud solutions reduce operational costs by streamlining IT management and minimizing the need for in-house technical staff (Misra & Doneria, 2018).

Cloud computing enhances the efficiency of financial operations by providing high-speed processing capabilities for large datasets and complex financial calculations. Real-time analytics, faster transaction processing, and improved decision-making are key advantages of cloud adoption. Cloud-based solutions also ensure global accessibility, enabling financial institutions to provide uninterrupted services to customers regardless of their location (Vadisetty, 2024).

Financial institutions are increasingly using cloud-based technologies such as AI, ML, and RPA to enhance risk management, fraud detection, and customer service. By automating routine tasks, banks can improve efficiency and allocate resources to more strategic initiatives. Cloud computing also fosters innovation by providing access to advanced development tools, allowing financial organizations to experiment with new services and optimize digital banking experiences (Литвин et al., 2024).

Financial institutions operate in a highly regulated environment, with strict guidelines on data security and privacy. Cloud providers offer compliance-ready infrastructures that align with industry regulations, enabling banks to meet legal requirements while maintaining operational efficiency. However, cloud migration requires careful risk management strategies, including robust encryption methods, secure access controls, and regulatory compliance audits. Financial organizations must work closely with cloud providers to ensure adherence to data protection laws across different jurisdictions (Misra & Doneria, 2018; Литвин et al., 2024).

Ensuring uninterrupted financial services is critical in the banking industry. Cloud computing enhances business continuity by providing disaster recovery solutions that minimize downtime during unexpected disruptions. Cloud-based backup systems enable rapid data restoration, ensuring operational resilience against cyber threats, natural disasters, or system failures. With geographically distributed data centers, cloud platforms offer redundancy and failover capabilities, safeguarding financial institutions from data loss (Vadisetty, 2024).

Cloud computing empowers financial institutions to offer personalized and seamless digital experiences to customers. Cloud-based CRM systems enable banks to analyze customer data and tailor financial products based on individual preferences. Additionally, cloud-based marketing platforms facilitate targeted communication through email, SMS, and social media, enhancing customer engagement. By utilizing cloud-driven insights, banks can provide proactive financial advice, loyalty programs, and customized investment options, ultimately improving customer satisfaction and retention (Литвин et al., 2024).

Despite its benefits, cloud computing presents several challenges for financial institutions. Data security concerns remain a significant barrier, as cloud storage introduces potential vulnerabilities compared to traditional on-premises systems. Reliability is another key issue, as financial services must be available at all times, even during extreme events or technical failures. Regulatory compliance complexities further complicate cloud adoption, requiring institutions to navigate different legal frameworks across regions. Lastly, managing multiple cloud vendors and ensuring seamless integration between cloud services requires strategic planning and robust IT governance (Misra & Doneria, 2018; Vadisetty, 2024).

As financial institutions continue to embrace cloud computing, the industry is set for further advancements in digital transformation. Future trends include the adoption of hybrid cloud models, edge computing for faster processing, and blockchain integration for enhanced security. By adopting these innovations, financial organizations can drive operational efficiencies, improve customer trust, and maintain a competitive advantage in a rapidly evolving financial landscape (Литвин et al., 2024).

Expected Evolution

The financial services industry has traditionally lagged in adopting cloud computing due to strict regulatory requirements, the complexity of legacy IT systems, and challenges related to data fragmentation. These factors have made financial institutions cautious about migrating sensitive data and critical operations to cloud environments. However, recent shifts in regulatory frameworks, along with growing recognition of cloud computing advantages, such as enhanced scalability, greater operational agility, and improved cost efficiency, have accelerated adoption of cloud computing in the financial

sector. Banks and other financial institutions increasingly embrace cloud technologies to modernize infrastructure and support innovative services (Chapman, Zaal & Kernahan, 2024).

Expansion of Cloud Computing

Cloud computing infrastructure is rapidly expanding and becoming more comprehensive across major commercial hubs worldwide. Leading cloud service providers now offer high bandwidth, optimized performance, compliance with local regulations, and robust disaster recovery capabilities. The increasing adoption of edge computing use cases has also driven cloud service providers to extend their coverage closer to data sources, though it is important to note that not all cloud services are available uniformly across all regions. First, initial foundational hubs are built in key continental technology centers, followed by additional hubs to improve global connectivity, and finally localized hubs are established in noncore and emerging markets (Galhardo-Burnett et al., 2023).

Despite a deceleration from 40% annualized revenue growth in mid-2021 to 28% in late 2022, cloud service providers continue to generate substantial revenues, around $50 billion quarterly. Projections indicate that total revenue could reach approximately $1 trillion by 2030. This growth is expected to follow an S-curve pattern typical of technological adoption cycles, suggesting that cloud computing remains in an early growth phase with significant potential to displace traditional on-premise data infrastructure (Galhardo-Burnett et al., 2023).

2.3.5 Internet of Things

IoT can be defined as a network of interconnected devices that collect and share data through the usage of sensors and other similar devices (Deloitte, 2021).

The integration of IoTs into the financial sector is revolutionizing banking services, security measures, and risk management. By enabling seamless communication between interconnected devices, IoT is enhancing financial operations through automation, real-time data collection, and advanced analytics. Financial institutions, under the right conditions, are using this technology to improve customer experience, optimize loan

management, strengthen cybersecurity, and introduce innovative payment solutions. However, while IoT presents significant opportunities, it also brings new challenges, particularly concerning data security and cyber threats (Johri et al., 2023; Tang, Huang & Wang, 2018).

IoT is playing an important role in modernizing banking services by enabling real-time data exchange between customers, financial institutions, and smart devices. Banks can use IoT to enhance customer interactions by providing instant account access, transaction alerts, and personalized banking services. The integration of biometric authentication, such as voice and touch recognition, further simplifies account management, ensuring secure and convenient access to financial services. Additionally, IoT helps banks optimize ATM deployment by analyzing usage patterns in different areas, ensuring better accessibility for customers while reducing operational costs (Johri et al., 2023; Suseendran et al., 2019).

Loan management is another area where IoT is making a significant impact. By collecting real-time data on borrower behavior, financial institutions can develop more accurate credit scoring models, leading to better lending decisions. IoT also enables banks to monitor the condition and usage of collateral assets such as vehicles, machinery, and real estate. GPS tracking and environmental sensors help ensure that collateral remains secure and within agreed-upon conditions, reducing the risk of asset mismanagement. Automated payment systems further streamline loan repayment by ensuring timely transactions, minimizing the likelihood of defaults (Johri et al., 2023; Rajput & Saxena, 2023).

If IoT devices have weak security, lack proper update mechanisms, or have no encryption, they can become major cybersecurity concerns, especially in financial institutions, where interconnected systems increase vulnerability to cyberattacks, data breaches, and fraud. Hackers can exploit weaknesses in IoT networks to gain unauthorized access to sensitive information. Unencrypted data, unsecured third-party services, and mobile banking vulnerabilities present significant risks that financial institutions must address through strong encryption, advanced authentication methods, and continuous security monitoring. The constantly evolving cyber threats show the necessity of proactive measures to prevent financial fraud, data theft, and unauthorized transactions (Choi & Lee, 2018; Rajput & Saxena, 2023).

IoT is also transforming payment systems by introducing automation and digital wallets. Through machine-to-machine communication, IoT facilitates seamless transactions between interconnected devices, enabling automated payments for various services. The concept of a "Wallet of Things" allows consumers to link multiple smart devices to their banking accounts, ensuring effortless financial transactions. However, as digital payment systems become more prevalent, financial institutions must implement stringent security protocols to protect against unauthorized access and fraudulent activities (Thirumagal et al., 2024; Suseendran et al., 2019).

The adoption of IoT in financial services extends to trade finance and risk mitigation. IoT-powered tracking systems monitor high-value goods in transit, ensuring the security of shipments and reducing the risk of financial losses. Radio Frequency Identification technology enables real-time monitoring of delicate goods, such as pharmaceuticals, allowing banks and insurers to make informed decisions regarding financial transactions and coverage. These advancements improve transparency in trade finance, ensuring that financial institutions can accurately assess risks and provide secure funding solutions (Tang, Huang & Wang, 2018; Rajput & Saxena, 2023).

Despite the benefits of IoT in financial services, challenges remain. The rapid growth of interconnected devices increases the complexity of managing security risks, regulatory compliance, and data privacy. Financial institutions must choose between technological innovation and risk management to protect customer data and maintain trust in digital banking solutions. Furthermore, the global disparity in digitalization levels means that some regions may face challenges in fully adopting IoT-powered financial services, necessitating targeted efforts to bridge the digital divide (Tang, Huang & Wang, 2018; Rajput & Saxena, 2023).

As financial institutions continue to embrace IoT, the future of banking will be shaped by automation, enhanced security, and improved customer experiences. The integration of IoT into financial operations presents opportunities for greater efficiency, better risk management, and innovative financial products. However, addressing cybersecurity threats and ensuring regulatory compliance will be essential to fully realize the potential of IoT in the financial sector (Johri et al., 2023; Tang, Huang & Wang, 2018).

2.3.6 Quantum Computing

Quantum computing is a technology that is currently in development and cannot be easily deployed. However, one can define it as a technology that utilizes quantum mechanics to perform complex calculations millions of times faster than normal computers. Unlike normal computers that use bits, quantum computers use qubits. Qubits are special because they have the properties of superposition, which allows them to exist in multiple states at the same time, and entanglement, which refers to their capability of linking two or more qubits where the change in one of them affects the others, which allows them to perform multiple tasks at the same time (Deloitte, n.d.).

Quantum computing is emerging as a transformative force in the financial sector, offering unprecedented computational power that has the potential to revolutionize risk analysis, portfolio optimization, fraud detection, high-frequency trading, and financial security. By using the principles of quantum mechanics, such as superposition and entanglement, quantum computers can process vast amounts of financial data at extraordinary speeds, uncovering patterns and solutions that classical computers struggle to identify. While the full-scale implementation of quantum computing in finance is still in its early stages, ongoing advancements indicate a future where financial institutions can significantly enhance decision-making, security, and efficiency (Akoh et al., 2024).

One of the most promising applications of quantum computing in finance is data analysis and pattern recognition. Financial institutions generate and process massive datasets, including market trends, customer transactions, and financial statements. QML algorithms, such as quantum clustering and quantum principal component analysis, enable a more sophisticated approach to data analysis, identifying patterns and anomalies with greater accuracy. These capabilities enhance fraud detection, market forecasting, and automated decision-making, allowing financial firms to operate with increased precision and reduced risk (Akoh et al., 2024).

In investment strategies, quantum computing offers superior portfolio optimization by rapidly evaluating numerous asset allocation combinations. Traditional optimization models often struggle with the exponential complexity of financial markets, whereas quantum algorithms can efficiently determine the best asset distribution to maximize returns while minimizing risk. This leads to enhanced investment strategies and improved

risk management, enabling financial institutions to construct more resilient portfolios (Akoh et al., 2024).

Risk assessment and option pricing are also key areas where quantum computing delivers significant advantages. The valuation of complex financial derivatives traditionally relies on Monte Carlo simulations, which are computationally intensive. Quantum Monte Carlo methods provide a faster and more accurate means of evaluating multiple risk scenarios simultaneously, improving the precision of derivative pricing models and enhancing market stability. Financial institutions can use these insights to make more informed trading decisions and mitigate potential losses (Akoh et al., 2024).

Another important application is in fraud detection and anti-money laundering. By utilizing quantum-enhanced ML, financial institutions can analyze vast transaction datasets to detect fraudulent activities with greater accuracy. Quantum algorithms identify hidden correlations and irregularities that traditional methods may overlook, reducing financial crime and strengthening regulatory compliance. The ability to process large volumes of transactional data in real-time significantly enhances security measures across banking and financial services (Akoh et al., 2024).

Quantum computing also has profound implications for HFT, where rapid decision-making is essential. Quantum algorithms enhance HFT strategies by analyzing real-time market data more efficiently, allowing traders to execute transactions with minimal latency. This leads to increased profitability and a competitive edge in fast-paced financial markets. By adopting quantum-enhanced pattern recognition, HFT systems can identify trading opportunities with greater speed and precision than classical algorithms (Akoh et al., 2024).

Financial security and cryptography are areas where quantum computing presents both opportunities and challenges. On one hand, quantum computers pose a threat to traditional encryption methods, such as RSA and elliptic curve cryptography, by efficiently solving complex mathematical problems that secure financial transactions today. On the other hand, quantum cryptography provides a solution through unbreakable encryption techniques like quantum key distribution. By ensuring secure communication channels and protecting sensitive financial data from cyber threats, quantum cryptography strengthens the overall security framework of the financial sector (Khang, 2025).

Regulatory compliance and ethical considerations also play a crucial role in the adoption of quantum computing in finance. Financial institutions operate within a heavily regulated environment, requiring stringent compliance with data protection and security standards. As quantum computing becomes more prevalent, regulatory bodies must adapt to address the unique challenges and risks associated with this technology. Additionally, ethical concerns, such as algorithmic biases and transparency in quantum-driven decision-making, must be carefully managed to ensure fairness and accountability in financial operations (Khang, 2025).

While quantum computing holds immense potential for transforming the financial sector, practical implementation remains in its early stages. The availability of high-qubit, stable quantum computers is still limited, and ongoing research is focused on overcoming hardware and scalability challenges. However, financial institutions, technology firms, and researchers are actively investing in the development of quantum solutions, paving the way for future breakthroughs (Khang, 2025).

As the field of quantum computing continues to evolve, its impact on finance will become increasingly significant. The ability to perform complex calculations at unprecedented speeds will drive advancements in risk assessment, investment optimization, market analysis, and security. While challenges remain, the financial sector is preparing for a future where quantum computing plays a central role in shaping innovative, data-driven financial strategies. Institutions that embrace this technological shift will be better positioned to use its advantages, ensuring greater efficiency, security, and competitiveness in the evolving financial landscape (Khang, 2025).

The Appearance of Quantum Computing

Estimates for the arrival of practical quantum computing vary widely depending on the pace of qubit growth and technological breakthroughs. A pessimistic outlook, assuming qubit numbers double every two years akin to classical Moore's law, projects that achieving 100,000 qubits would likely occur well beyond 2040. On the contrary, an optimistic scenario, highlighted by IBM's recent advancements with qubit counts doubling approximately every nine months, suggests that practical quantum applications requiring fewer than a million qubits could emerge as soon as 2030. An intermediate perspective, which assumes an annual doubling of qubits and reflects expert consensus,

anticipates useful quantum computing capabilities for complex tasks like quantum chemistry simulations and cryptographic codebreaking between 2033 and 2040. However, qubit quantity alone is not sufficient to realize the full utility of quantum computers, advancements in quantum algorithms, error correction techniques, hardware fidelity, and ancillary technologies are equally vital. Despite these challenges, the first practical quantum applications are broadly expected around 2035, though significant uncertainty remains given the complexity and interdependence of the required technological progress (Groenland, 2025).

Expected Cryptography

Asymmetric encryption currently underpins the security of sensitive digital communications, such as online transactions, relying on the computational difficulty of reversing encryption keys with classical computers. However, the advent of powerful quantum computers threatens this security paradigm, as these machines could efficiently break widely used encryption schemes. Although building such quantum systems is expected to be extremely expensive and likely limited to nation-states targeting highly valuable information, especially national security data, the primary concern lies in the "store-and-break" threat. This risk involves adversaries intercepting and storing encrypted data today, only to decrypt it in the future once quantum capabilities mature, thus threatening the confidentiality of information that requires long-term protection. Quantum attacks are expected to be deliberate and sequential, beginning with the most valuable data, making proactive adaptation essential to maintain security. Developing and deploying quantum-resistant cryptographic methods is therefore important to safeguarding both current and future communications (Scholl, 2021).

Given the approximation of the threats posed by quantum computing, organizations are urged not to delay action until formal standards are finalized. Instead, they should immediately identify their most sensitive data and evaluate its vulnerability to quantum attacks. Prioritizing the transition to quantum-resistant encryption for valuable information as part of broader infrastructure upgrades is essential in the coming years (Scholl, 2021).

2.3.7 Neurocomputing

Currently, the main applications of neurocomputing currently focus on areas requiring efficient and parallel processing of large, complex datasets. These include pattern recognition, image analysis and interpretation, robotics, autonomous systems, and advanced AI models such as deep learning and reinforcement learning. Neurocomputing systems are also being explored for use in real-time decision-making tasks, adaptive control systems, and enhancing the energy efficiency of AI computations (Intel, 2021; Schuman et al., 2017).

There is still limited information about neurocomputing, but it's possible to find growing indicators of advancements in this technology. For example, Intel recently developed some progress in this field, particularly with the introduction of their new next-generation neuromorphic research chip, which is designed to mimic the architecture and functionality of the human brain (Intel, 2021).

2.3.8 Application Programming Interface

APIs are essential to open banking, enabling secure and standardized data sharing between financial institutions and third-party providers. They support innovation in services like payments and lending but also introduce serious security risks. Poor API design can lead to data breaches, unauthorized access, and DoS attacks. Weak authentication remains a top concern, and most organizations have faced API-related security incidents. Risks from third-party providers further complicate the threat landscape. To mitigate these issues, experts recommend strong authentication, thorough vetting of external partners, traffic monitoring, and rate limiting (Hossain, Raza & Rahman, 2025).

Expected Evolution

APIs are extremely important to open banking, enabling innovation and collaboration between financial institutions and third-party providers. However, they also introduce significant cybersecurity risks. To address these, institutions must adopt secure coding practices, follow security guidelines, and implement advanced security measures like API gateways, behavioral analytics, and multifactor authentication. Regular testing, rate

limiting, and monitoring are essential for maintaining system integrity (Hossain, Raza & Rahman, 2025).

Managing third-party risk is very important, requiring strong contracts and regular audits to ensure compliance with security standards. Additionally, training stakeholders through seminars and real-world simulations improves awareness and preparedness against API threats. Overall, a layered, collaborative approach is vital for building a secure and resilient open banking environment (Hossain, Raza & Rahman, 2025).

Third Payment Services Directive

The introduction of the revised PSD3 marks a significant regulatory advancement for both traditional banks and non-bank Payment Service Providers across applicable jurisdictions. By expanding the regulatory framework to include a broader range of actors, PSD3 aims to level the competitive landscape while ensuring greater consumer protection and service consistency across all payment providers. This broader inclusion is intended to drive fairness and regulatory cohesion in the evolving digital financial ecosystem (J.P. Morgan, 2024).

In the context of open banking, PSD3 represents a key evolution in how APIs are standardized and governed. Among its most impactful provisions are the establishment of stricter functional and performance requirements for APIs, the obligation for open banking entities to provide user-accessible monitoring dashboards, and enhanced transparency mandates. These measures are intended to solidify trust and usability within the open banking space by ensuring that APIs deliver reliable, secure, and user-friendly interactions (J.P. Morgan, 2024).

Moreover, organizations that act early to adopt PSD3-aligned open banking solutions are poised to benefit from operational efficiencies and competitive differentiation. Enhanced security through improved API interfaces enables better payment authentication and validation, while greater visibility into transaction flows fosters trust and risk mitigation. Together, these advancements contribute to the emergence of a more seamless, efficient, and resilient digital payment infrastructure (J.P. Morgan, 2024).

2.3.9 Robotic Process Automation

RPA has experienced significant evolution, shifting from rudimentary hardware-based automation towards sophisticated software systems that emulate human interaction with digital environments. Early iterations of RPA were primarily focused on automating straightforward tasks, such as data entry and routine data manipulation, relying on fundamental techniques like screen scraping and data extraction to interface with legacy software systems. These foundational methods allowed RPA bots to replicate user actions, enabling automation of repetitive and rule-based activities (Pandy et al., 2024).

As RPA technology progressed, its capabilities expanded substantially through the integration of AI and ML. This fusion led to the emergence of intelligent automation, which combines traditional RPA with AI-powered functionalities. Intelligent automation utilizes ML algorithms and natural language processing to execute tasks, provide data-driven insights, and optimize workflows. Consequently, RPA has transitioned from simply automating manual tasks to enhancing decision-making processes and managing more complex, cognitive activities. This evolution broadens the scope and impact of RPA across various industries, enabling organizations to achieve higher efficiency and productivity by automating increasingly sophisticated business processes (Pandy et al., 2024).

Optical Character Recognition

OCR technology has evolved from early template matching and rule-based methods, which struggled with handwriting, complex fonts, and distorted images. These traditional systems required high-quality inputs and had limited accuracy (Shekhar, 2025).

The major breakthrough came with deep learning. Convolutional Neural Networks improved image processing, enabling accurate text recognition even in noisy or low-resolution images. Recurrent Neural Networks, especially LSTM networks, helped OCR handle sequential data like handwriting and video text. Deep learning OCR systems are more robust, performing well under varied lighting, noisy backgrounds, and complex images. This marked a significant improvement over earlier methods (Shekhar, 2025).

Integrating natural language processing further enhances OCR by enabling contextual understanding, error correction, and better text interpretation. AI-powered OCR can now grasp not just text, but also its meaning within larger contexts. Overall, combining deep

learning and NLP has greatly increased OCR's accuracy and flexibility for real-world applications (Shekhar, 2025).

2.4 Regulatory Responses and Challenges

Currently, regulators tend to wait until a technology reaches a certain adoption or risk level before intervening, possibly to avoid overregulation or misjudging its impact. However, this reactive attitude may prove problematic in a future where technological innovation may occur at a never seen speed and scale. As a result, regulators may struggle to keep pace with more complex evolutions of technologies such as AI, smart contracts, and algorithmic trading. These innovations, if left unregulated or loosely regulated, could lead to systemic risks, especially when they become more adopted into the core operations of the financial sector. The inability to anticipate and manage such risks may in turn lead to financial instability, particularly if the regulatory response remains fragmented or outdated (Taylor et al., 2020; Ahern, 2025).

As financial technologies evolve, existing legal definitions and frameworks have the possibility of becoming obsolete or misaligned with market environments. This could either suppress innovation through excessive constraints or leave dangerous gaps where harmful practices can occur. A significant structural issue is the reliance on rigid legal classifications that cannot keep up with the technological adaptability of modern financial instruments. A function-based regulatory model focusing on the risks and economic functions of activities, rather than their formal legal categories, is needed, especially given innovations like tokenization and DeFi. Without this approach, legislation may either overregulate and stifle innovation or underregulate and leave systemic threats unaddressed (Ahern, 2021).

Although the EU has taken steps through initiatives like MiCA, DORA, and the DLT Pilot Regime, regulatory fragmentation across jurisdictions remains a challenge. Institutions must navigate multiple overlapping regulatory regimes, leading to compliance inefficiencies and raising the risk of avoiding regulations. Coordinating regulatory approaches internationally will become more difficult, especially for technologies like DeFi or cloud computing that defy geographical barriers (Deloitte, 2024; Zhang et al., 2019).

Finding the right balance between fostering innovation and managing risk is becoming increasingly complex. Overregulation could harm the development and deployment of new financial technologies, while underregulation might expose consumers and institutions to cyber threats, fraud, and systemic failures. Experimental regulatory approaches such as innovation hubs and regulatory sandboxes have proven effective by allowing regulators to understand new technologies better and giving firms a controlled environment to test compliance. Early regulatory engagement during the development of technologies also contributes to more informed and effective policy outcomes (Zhang et al., 2019; Taylor et al., 2020).

The growing digitization of financial processes brings heightened cybersecurity risks. Technologies like AI can strengthen security but also become new targets for exploits. Regulatory frameworks, such as those outlined in DORA, will need to continuously evolve to address these threats without overburdening smaller institutions that cannot fully comply with them (Tartaro, Smith & Shaw, 2023; Deloitte, 2024).

Data privacy and information governance present additional challenges. While data-driven innovation depends on broad access to high-quality information, stricter privacy regulations can introduce bureaucratic obstacles and reduce the availability of usable data. This situation leads to increased compliance complexity, higher costs, and potential reduction of innovation (Tartaro, Smith & Shaw, 2023).

Finally, regulatory institutions must be prepared for the future by investing in advanced analytical tools and simulation models to detect risks and design appropriate responses. However, public regulatory agencies often struggle to attract and retain technical talent due to salary competition from the private sector. Additionally, the complexity of algorithmic and AI-driven systems demands specialized evaluation methods that many regulatory bodies have yet to develop, threatening their ability to respond effectively to rapid technological transformations (Ahern, 2025; Tartaro, Smith & Shaw, 2023).

3. Methodology

This study employs qualitative research, utilizing both primary and secondary data sources. The primary data were collected through semi-structured interviews, while the secondary data were gathered from peer-reviewed literature and other institutional sources.

The semi-structured interviews were conducted with experts selected through a selective sampling, based on their specialization in areas related to the financial sector, information systems, and/or emerging technologies. These interviews aimed to gather in-depth insights from experts directly involved in dealing with technology adoption and strategy in financial institutions. The interviews were either conducted in person or online, with all recordings being done with the participants' consent, and then subsequently transcribed for analysis. Secondary data were gathered from academic databases such as, but not limited to, Google Scholar and b-on, including journals, articles, videos, conference papers, regulatory documents, interviews, and technical reports. The literature review follows topics such as emerging technology, financial regulation, evolution of technology, evolution of the financial sector, technology adoption in the financial sector, and financial regulations, which then led to the research on AI, ML, blockchain, cloud computing, IoT, cybersecurity, quantum computing, and after completely analyzing the results from the interviews additional topics such as neurocomputing, DLT, API, and RPA.

The interview transcripts were analyzed using a thematic analysis, involving familiarization with the data, initial coding, and grouping codes into broader themes. Codes were based on both the type of technology discussed and the confidence in the responses. These themes were then aligned with the research questions to be able to answer them.

The literature was reviewed so as to identify how current academic perspectives support or contrast with the experts' interviews. This leads to a reduction in the possibility of biased conclusions, or answers being influenced by professional constraints, while also leading to the analysis of different perspectives.

During this research all participants were informed about the research objectives and how their data would be used. All personal information has been anonymized, except

where participants explicitly consent to its disclosure, and all data were stored securely to ensure confidentiality.

4. Research Results

4.1 Artificial Intelligence

The data from the interviews indicates that AI is currently being implemented in multiple areas of the financial sector. It was reported that it is being heavily utilized in capital markets, in algorithmic trading, in banking, particularly in payment-related projects, and in insurance, to support insurance mediators. ML, an important part of AI, is usually applied in tasks such as credit scoring, creditworthiness evaluation, and repayment prediction, usually accompanied by human oversight.

AI has an important role in the process of automation, including customer service automation and self-service transaction interfaces, and is increasingly used to improve operational efficiency, which was described as a primary focus of AI applications. Even still, there is an ongoing challenge of enhancing service efficiency and personalization through AI without compromising user privacy or dehumanizing the customer experience. As such, choosing technologies and suppliers that uphold strong privacy standards has become a very important step in the application of AI.

There is deliberate caution in the implementation of AI, particularly in areas involving trust and customer relations, which are currently mainly handled by humans. As such, most institutions try to ensure that AI only receives non-personal and generic data. For now, institutions are still waiting for AI to improve before a broader exposure to clients.

Emerging tools like CoPilot and ChatGPT were mentioned as supporting information gathering, creative processes, and decision-making, especially in internal meetings, where they help reduce time and increase efficiency. These tools also contribute to collaboration, rapid discovery, and information consolidation. Some institutions noted that their internal teams are developing software with the help of generative AI, especially during the programming phase.

Although its current implementations are widespread, there is an expectation for further development, and potential to broaden opportunities for firms and investors. With special mention of its roles in early fraud detection, pattern recognition, and scalable deployment. Still, one interviewee lately referred that there aren't any significant innovations or novel phenomena at least within the financial market.

In risk and fraud detection, AI must remain unbiased and resistant to manipulation. To accomplish that, it requires a careful selection of technology and database suppliers, run reoccurring performance evaluations, and avoid the use of generative AI in its core businesses. Even still, to truly guarantee the accuracy of the results, these processes are usually managed by humans.

Concerns were raised regarding AI transparency, particularly due to the "black box" nature of its models. One interviewee noted that currently there is a lack of a unified framework for testing and validating AI systems. In terms of regulation, the recently published EU AI Act was identified as an important step toward increasing oversight and accountability, though it was also described as very new and still under development.

It was referred that it is hard to know how technology might evolve, due to being almost like a prediction. Nevertheless, many technologies may change in the following years, but none will be as disruptive as AI. It was stated that technology will modify our future and the way we do business today, some even declared that a change in the way investors, customers, policyholders, and firms interact with technology would occur in the next 5 to 10 years, however, no one seemed to know entirely how.

Even still, some stated that AI will see an increased use, and it may evolve so as to enhance client interaction, increase the speed and quality of the service, improve and expand applications in fraud detection, and enhance risk evaluation capabilities. Additionally, AI will play a more significant role in workforce management. Meanwhile, some expect the reduction of intermediaries, allowing consumers and investors more direct access to service providers and the services themselves. Even though this might lead to faster and more efficient processes, it might also cause a reduction in caution and an increase in dehumanization of processes when dealing with customers. One expert noted that many of the anticipated developments mentioned earlier in this paragraph could also apply to blockchain.

Looking even further ahead, AI may also enable greater personalization by developing models that adapt to the unique needs of individual customers. One expert noted that many of the anticipated developments mentioned earlier in this paragraph could also apply to blockchain.

The quality of ML only depends on the quality of its data. As such, ensuring quality data becomes one of the most important factors in maintaining a proper ML system, and

to ensure that, proper control systems must be used. It was stated that most problems related to AI and ML can be avoided if the control system are done by humans instead of machines, and the results aren't followed blindly.

Some expect that in the future, the difference between institutions will be seen in who has the best regulators, the better trained staff, and only utilizes AI and ML as tools to help in human decisions.

All of this has led the experts to anticipate a growing number of professionals well-trained in AI technologies, cloud computing, and related fields, due to an expected rise in demand from institutions. With the anticipated increase in the number of applications and capabilities of AI, some are led to believe that there might occur an increase in biases, especially if its processes are not well managed. The increased and more general use of AI by institutions may bring more risk, more specifically systemic risks. These includes the obsolescence of current models and heightened cybersecurity threats. During periods of stress, reliance on similar or equal models could further boost market instability.

It has been expressed the belief of an increase in the acquisition of private data and information by institutions leading to possible privacy issues and becoming more likely targets of cyber-attacks. As such, it's expected an increase in investment in cybersecurity and data protection.

Currently, in the AI act, rules and regulations related to the possibility of companies relying entirely on AI-generated information remains a subject of ongoing debate. In the financial sector, two specific applications of AI are currently considered as high risk: the usage of AI for credit risk assessment and the processing of sensitive personal data by insurance companies. Still, the future direction and scope of the AI act remain uncertain.

The possible wide adoption of similar AI systems can lead to similar results. Consequently, the widespread adoption of those AI-generated responses, including the usage of ML in predictive analysis, may contribute to increased market volatility, heightened systemic risk, the emergence of sudden market spikes, and reduced diversity. Meanwhile, one expert declares that AI and ML will have great difficulty predicting results with high enough levels of confidence that it becomes a problem, making this risk less problematic or less likely to occur.

The ability of AI systems to explain their logic and processes still remains quite underdeveloped. This lack of explainability presents a challenge, especially when transparency and accountability are most important. This can sometimes make AI seem unreliable, leading to the production of inaccurate or misleading information, which can negatively affect the trust in its answers. Accentuating the ongoing need for human management to ensure the quality and appropriateness of responses, especially in main business operations and customer interactions, where the accuracy and respectfulness of the communications are essential. On the contrary, one interviewee explained that in low-risk applications, such as image generation, such intensive surveillance may not be necessary, as the consequences of errors are usually minor.

Some companies are reluctant to fully adopt AI and ML for decision making and forecasting. While some other companies believe that AI can replace the human role, in these companies, the evolution of technology could lead to an increase in layoffs.

4.2 Blockchain

Interviewees reported that blockchain is already associated with crypto assets, which are currently being regulated as financial instruments. Several noted that blockchain is being studied for use in traditional financial markets, including by clearing systems, securities depositories, and trading platforms. Blockchain is also applied in payments-related projects within banking.

Usage examples include cryptocurrency transactions and validation of financial institution contracts. Some interviewees highlighted that insurance contracts for logistics operators have been implemented using blockchain, and that blockchain is used by insurers for B2B insurance purposes. Additionally, neobanks have adopted blockchain, benefiting from its support for digital customer interactions.

Some interviewees indicated that the cryptocurrency sector is monitored by banks but not actively used, and that blockchain is not widely adopted by retail banks. It was stated there are insufficient use cases for broader adoption by banks, with traditional banks tending not to adopt blockchain at this time.

Barriers to adoption include the need for specialized training and the perception that blockchain providers do not offer sufficiently attractive services for banks. Hesitation also

arises due to blockchain's lack of full process transparency and fluidity, which some interviewees identified as obstacles to wider implementation.

The potential for blockchain to create efficiencies and reduce intermediaries in capital markets was acknowledged, and the payments sector is reported to be undergoing significant changes due to blockchain.

4.3 Cloud Computing

Cloud computing is currently mainly implemented in the financial sector for document management, data lakes, and various cloud-based services, with its usage expected to continue increasing. Many banks began transitioning to cloud infrastructure between 2015 and 2020, and adoption rates vary across organizations. Cloud platforms such as Azure Databricks are widely used and considered important tools.

The shift to cloud computing enables faster innovation by removing the need for local infrastructure and allows financial institutions to rapidly scale their service capacity. It also supports reporting services by facilitating efficient information acquisition. The growing influence of AI and Big Data is driving further demand for cloud services, likely transforming business models in the near future.

Despite these advantages, concerns remain around cybersecurity risks unique to cloud environments, such as DDoS attacks. Additionally, reliance on third-party providers can reduce flexibility and introduce operational risks, making risk management and provider diversification essential for maintaining service continuity.

Cloud computing usage is expected to increase over the year, with the possibility for a reduction of its price or the expansion of the services of large providers geographically in the following years. It was referred by one expert that it will continue to evolve primarily as a "bridge" between technologies.

Currently, cloud Computing usage and applications in EU are being managed by DORA, through the issuing of guidelines for financial institutions.

Adopting an universal regulation for cloud computing presents significant challenges. Because of that, regulatory discussions primarily occur through communication between authorities and international forums. The existence of different methods of data management in distinct authorities is one of the biggest barriers to a worldwide general

regulatory framework. These differences may include distinct protocols for reporting cyberattacks and other incidents, as well as divergent procedures for recovery and response following such events. Additionally, differences in cybersecurity regulatory approaches across jurisdictions may create further complexity, harming this global adoption. Lastly, existing regulatory instruments may often contain gaps that hinder the development of comprehensive and cohesive cloud computing regulations.

Some experts refer that due to the absence of standardized legislation, the risks associated with cloud computing can vary significantly across regions. One expert even stated that these risks may include fluctuations in pricing, differences in the underlying legal frameworks and compliance obligations, and exposure to geopolitical tensions. Companies may also face unexpected tariffs or regulatory changes that affect the operation and cost-efficiency of cloud services. For financial institutions, it became essential to ensure that the cloud service providers comply with the regulatory requirements set by domestic and international supervisory authorities.

4.4 Internet of Things

One interviewee indicated that IoT technologies are currently used in ATMs and other machines to monitor maintenance needs. It was also referred that currently, there exists the technology to utilize sensors to identify customers entering bank branches through customers' mobile phones. However, this type of IoT adoption remains limited, as the technology is still largely in the prototype stage, with many expressing high caution due to privacy concerns.

4.5 Quantum Computing

Interviewees reported that although the banking sector is aware of the existence of quantum computing, it has seen very limited adoption, particularly in Portugal. Although some respondents acknowledged potential future applications in areas such as risk assessment, the current use cases are neither well-defined nor operationalized. Currently, there are no significant implementations demonstrating clear gains in efficiency or other measurable benefits. The high costs associated with implementation and maintenance were consistently cited as major barriers, making it difficult for institutions to justify

investing in this technology at this stage. Some experts expressed that in the next five to ten years, there is a possibility for a wider adoption of quantum computing, however the majority of the experts don't agree with this affirmation, stating that even then it would still be too early. One expert even references the possible emergence of neurocomputing, which is a technology that tries to replicate the structure and functions of the human brain. Neurocomputing is already being worked on, however, it currently still needs further development. One of the experts expects that neurocomputing will not become avaiable for implementation in any sector within 10 years.

One expert expressed concern that future advancements in quantum computing could pose a threat to the security of blockchain systems, potentially making current cryptocurrency infrastructures vulnerable to cyber attacks. This would challenge the perception of cryptocurrencies as inherently secure. Nonetheless, it was also stated that the decentralized nature of these systems provides a degree of resilience, acting as a built-in security feature. Another expert, while stating that there is a high chance of future encryption threats, it is still too early to know how it will truly affect blockchains cryptography.

Despite the possibility of these risks, it is anticipated that the market, including both users and developers, will respond with new protective measures. It was suggested that, much like the evolution of internet security, blockchain systems would likely adapt over time to address emerging threats. However, in the end, the responsibility for safeguarding these systems will rest with both the technology's developers and its users.

4.6 Application Programming Interface

One interviewee highlighted that APIs are the most utilized technology in the financial sector nowadays, being mainly utilized to connect on-premise systems with cloud infrastructure, facilitating integration across technological environments. It has also been referred that PSD2 is currently being updated to incorporate enhanced API security. Looking ahead, PSD2 is expected to evolve into PSD3, which is anticipated to bring improvements in security and updated regulatory standards for API usage in the financial sector.

Currently some are led to believe that API is reaching its peak performance, and it shouldn't improve or evolve much more than its current state.

4.7 Robotic Process Automation

One interviewee noted that RPA is currently used for process automation, particularly to automatically read digital documents and to scan and convert physical documents into digital formats. In Portugal, RPA adoption became widespread only recently, with significant uptake occurring around 2020 or 2021.

Some anticipate that the number of RPA processes required to operate the technology will decrease over time, with expectations that this trend will continue in the coming years. This would allow for the same output to be achieved with even less input, thereby increasing overall efficiency. Additionally, RPA is expected to see improvements in its OCR capabilities, enhancing its ability to process and extract information from data sources. It has also been noted that the effectiveness of RPA can vary depending on how it is implemented and applied.

4.8 Distributed Ledger Technology

One Interviewee briefly referred to the importance of the usage of DLT for monitoring purposes, with a particularly high adoption in the cryptocurrency sector. Additionally, institutions are collaborating with policymakers to ensure that the use of DLT supports investor protection and maintains financial stability.

4.9 Legacy Systems

Some interviewees emphasized that financial institutions often rely on a mix of technologies, combining systems that are over 20 years old with newer solutions to compensate for their missing functionalities, however this integration requires specific components that link traditional systems to newer systems.

Such integrations can result in the reduction of data richness, which leads to the loss of detail of the data. Security concerns may also arise due to the lack of authentication mechanisms in older systems.

It was also noted that the financial sector adopts new technologies more slowly than other industries, such as retail. Within the sector, the insurance industry lags behind in

adopting innovations like AI and cloud computing. Furthermore, institutions tend to be more cautious when implementing emerging technologies in core business areas, which reduces the speed and scale of adoption.

4.10 Regulation

4.10.1 Digital Finance Pack

In 2020, the European Union introduced the Digital Finance Package, which comprises three legislative diplomas.

4.10.1.1 Markets in Crypto-Assets Regulaction

MiCA aims to address crypto assets that were previously outside the scope of existing financial legislation, more specifically, those that do not qualify as securities, financial instruments, deposits, or insurance products. Meaning that MiCA targets crypto assets that existed in "no man's land". According to the interviewee, MiCA addresses this gap in two primary ways. First, it treats certain crypto assets in a manner similar to traditional securities, introducing transparency requirements for service providers and issuers. These obligations aim to improve market functioning, protect investors, and address information asymmetry, which is a key market failure identified by both crypto-asset investors and issuers or service providers. Second, the regulation also focuses on stablecoins, or crypto assets designed to maintain a stable value. These assets create potential risks to financial stability and monetary policy, especially due to their potential widespread use as means of payment. As such, MiCA proposes regulating stablecoins as payment instruments, including placing limits on their scale, especially if they introduce alternative units of account or challenge the Euro and other official EU currencies.

4.10.1.2 Distributed Ledger Technology Pilot Regime

Regulation on a Pilot Regime for market infrastructures based on distributed ledger technology, which aims to explore how blockchain technology can be integrated into financial markets. This regulation also establishes a time-limited test regime that allows entities to experiment with blockchain-based solutions for trading and settlement

systems of financial instruments. This framework includes legal exemptions to determine whether existing legal or operational barriers hinder the development of blockchain applications in market infrastructure. It also seeks to test the capability of reducing the number of intermediaries, by relaxing legal requirements that currently mandate their involvement, to assess whether markets can function more efficiently with fewer intermediaries. An evaluation report by ESMA is expected in 2026, which will help determine whether this regime should be continued, revised, or terminated. However, no major new regulatory responses are anticipated in Europe in the short term, but it is anticipated that starting next year, regulators will begin to consider whether revisions to the existing legislation may be necessary inthe medium to long term.

4.10.1.3 Digital Operational Resiliance Act

DORA addresses cybersecurity within the financial sector by establishing specific standards that align with the EU's broader cybersecurity framework, known as NIS2. It hopes to create a stronger security regime for financial institutions by creating duties for all entities to prevent cyber risk incidents.

4.10.1.4 International Influence of the EU Digital Finance Package

In the rest of the world, it is not yet clear whether similar frameworks will be implemented as in the EU. However, there seems to be a strong tendency for non-EU countries to build regulatory frameworks already established in the EU. Much like what happened with the GDPR, where many jurisdictions adopted or adapted its principles into their own legal systems, it has been referred in an interview that the same is to be expected to occur with the EU's digital finance package. For example, the United Kingdom has already implemented a regulatory sandbox that is very similar to the EU's DLT Pilot Regime. In the United States, ongoing discussions about extended legislation for crypto assets are also likely to be influenced by MiCA. However, one expert stated that it is to be expected that each country's regulations will evolve differently.

4.10.2 Regulation in Times of Crisis

In times of crisis, regulatory institutions, such as central banks, act immediately to contain it, while conducting advanced research and scenario planning to improve future responses to a crisis or unforeseen disruptions.

4.10.3 Regulatory approach to emerging Technologies

According to some interviewees, regulations related to technologies usually appear only once those technologies become widely adopted. When a technology is not yet widely adopted, there is often a small need for legislation. In other words, rather than proactively anticipating the implications of emerging technologies, regulatory approaches tend to be reactive, leading to legislation being introduced only after the technology and its consequences occur. In the development of those new regulations, it is first observed the market developments and responses. Then it's analyzed how, where, and when intervention is necessary, through the engagement with investors, consumers, firms, other regulatory bodies, and academic experts.

While regulation usually comes after the adoption of technology, according to one expert, financial institutions, such as banks, should be proactive when it comes to technological innovation. As embracing a reactive attitude may lead to missed opportunities.

Despite the need for regulation to address emerging risks, some experts stated that regulations should not hinder the adoption and use of technology. While greater risks justify the increased need for stronger supervision, it is essential to preserve the innovation of institutions. As technology continues to evolve, there is a possibility that existing legislation may become outdated or redundant. Therefore, a balance must be struck between imposing necessary restrictions and allowing for technological progress, ensuring that legal frameworks do not cease innovation within companies.

Nonetheless, one interviewee noted the possibility of an increase in data privacy regulation, which is likely going to make the use of data and information in applications

and processes more challenging, due to more intensive bureaucratic requirements for data access and a reduction in the availability of accessible information.

It was stated that it is considered very important to remain prepared to address emerging risks, even though the exact nature of these risks is currently unknown. This can be achieved by accepting the introduction of new regulatory requirements, such as updated recording formats, and continuous evaluation of existing requirements to determine whether they should be maintained, modified, or removed.

5. Discussion

Question 1: Currently, what are the main emerging technologies being applied in the financial sector, where are they being applied, and what implications do they bring?

Institutions of the financial sector tend to adopt new technologies more slowly than institutions from other sectors, and within the sector, the insurance industry is even slower. Furthermore, institutions tend to be more cautious when implementing emerging technologies in core business areas. However, according to the results of this study, the current most important and most applied emergent technologies in the financial sector are AI, ML, Blockchain, Cloud Computing, API, RPA, and DLT. IoT can still be considered an important technology, especially for real-time monitoring and data collection, however it is not as widely used due to its several security and privacy risks.

Artificial Intelligence

AI is the most prominent emerging technology currently applied across the financial sector. Its presence covers various segments, including capital markets, banking, insurance, risk management, and customer service. The technology's growing importance is largely tied to its capacity to improve operational efficiency, decision-making, and service delivery through automation and data-driven insights.

In capital markets, AI is being utilized for algorithmic trading, enabling faster, more accurate transactions while identifying complex market trends in real time. In banking, AI streamlines payment processing and accelerates procedures such as loan approvals. While in insurance, it supports claims handling and underwriting by improving the speed and consistency of assessments. These improvements result in both increased customer satisfaction and cost reductions.

Another major application of AI is in credit analysis and risk evaluation. ML models are increasingly used to generate more precise credit scores by analyzing a broader range of behavioral and contextual data, extending access to credit while improving risk assessments. AI is also heavily utilized into fraud detection systems, by utilizing its pattern recognition capabilities and real-time monitoring AI can flag unusual transactions earlier.

Customer service has also seen significant transformation through AI. The implementation of chatbots, virtual assistants, and other self-service platforms improves responsiveness and reduces operational costs. However, these gains come with trade-offs. As automation increases, there is some loss of personalized, human-centered service. Institutions often respond by integrating AI selectively in customer-facing roles, balancing efficiency with the need for trust and human interaction.

Internally, AI tools such as ChatGPT and Copilot are beginning to assist teams with communication, creative problem-solving, and even coding tasks. This proves theAI's role not only in external service delivery but also in enhancing internal productivity.

Despite the benefits, challenges such as lack of transparency remain. AI systems often function as "black boxes" making it difficult to trace or explain decision-making processes, this creates regulatory and trust-related concerns, particularly in areas involving personal data. In response, many financial institutions are limiting AI applications to non-personal or generic data while maintaining human oversight, especially in high-risk operations like fraud detection and credit scoring. Additionally, issues of bias, data privacy, and ethical accountability are some of the most prominent current challenges that require continuous monitoring.

Blockchain

The most visible and established application of blockchain is in cryptocurrency, where it serves as the foundational infrastructure enabling decentralized transactions. However, beyond cryptocurrencies, broader implementation of blockchain remains limited, especially among traditional retail banks.

In the insurance sector, blockchain is being explored in specific B2B applications, such as automating insurance contracts for logistics operators. These use cases utilize blockchain's ability to provide transparent, tamper-proof records and smart contract execution to improve operational efficiency and trust among parties.

Within banking, the application of blockchain is more cautious. Traditional banks are closely monitoring its developments in crypto but tend to avoid using blockchain outside of some payments-related initiatives. One of the main factors currently limiting this adoption is the perception that existing blockchain solutions do not offer a strong enough

value proposition to justify widespread investment. Moreover, the current integration of blockchain systems with legacy infrastructure poses significant technical and organizational challenges, particularly concerning interoperability, transparency, and real-time visibility.

Another practical barrier is the need for specialized training to develop in-house blockchain expertise. For many institutions, the investment in talent and infrastructure is not yet justified by the current business use cases available. In contrast, neobanks and digital-first institutions are more inclined to adopt blockchain due to their technological agility and alignment with blockchain's decentralized, always-online nature.

Despite these limitations, blockchain does hold transformative potential. Its core strengths offer significant advantages in use cases like fraud prevention, auditability, smart contracts, and cross-border payments. Furthermore, DeFi platforms demonstrate how blockchain can disrupt traditional financial models by enabling peer-to-peer transactions without intermediaries, reducing costs and increasing speed. Still, decentralization also introduces new challenges, particularly in regulatory compliance, transaction monitoring, and enforcement of legal standards. Financial institutions and regulators must understand how to manage and supervise blockchain systems while preserving their core decentralized nature. These concerns are amplified by technical risks such as smart contract vulnerabilities, 51% attacks, and private key mismanagement.

In summary, while blockchain's promise is widely acknowledged, its current application in the financial sector remains selective and experimental, largely constrained by integration difficulties, regulatory uncertainties, and the still-maturing ecosystem. Nonetheless, digital-native financial institutions and niche insurance applications are laying the groundwork for broader adoption in the future, especially as interoperability and regulatory clarity improve.

Cloud Computing

Cloud computing has become widely adopted for document management, data lakes, and diverse cloud-based services. Platforms such as Azure Databricks are recognized as critical tools that support data processing and analytics capabilities across financial institutions.

The transitions to cloud infrastructure among many banks began around 2015–2020 and continue to occur today. The current broader adoption of this technology is due to its capability to eliminate the dependence on local infrastructure and allowing organizations to rapidly scale service capacity, enhance operational agility, and improve information acquisition. However, the migration to cloud computing is not without challenges. Cybersecurity risks, such as DDoS attacks, and operational vulnerabilities, related to the reliance on third-party cloud service providers, are still some possible concerns.

When applied cloud computing can enhance efficiency by providing scalable computing power to handle large datasets and complex financial calculations, facilitating real-time analytics and faster transaction processing. It supports cost-effective operations by reducing capital expenditure on hardware and allowing a pay-as-you-go model, freeing resources to invest in innovation and customer experience improvements.

Cloud platforms also bolster security through encryption, multi-factor authentication, and strict access controls, alongside real-time threat detection capabilities. These features help financial institutions protect sensitive customer data and comply with regulatory requirements across jurisdictions. Additionally, cloud-based disaster recovery and backup solutions can improve business continuity by ensuring rapid data restoration and minimizing downtime during disruptions.

Financial organizations are increasingly combining cloud computing with technologies such as AI, ML, and RPA to enhance risk management, fraud detection, and customer service. Cloud computing infrastructures provide the flexibility and computational power necessary to deploy these tools, allowing the automation of routine tasks and enabling teams to focus on more strategic priorities.

Despite its clear benefits, the adoption of cloud computing in finance requires ongoing attention to data privacy, regulatory compliance, and governance complexities. Institutions must develop comprehensive strategies to manage multi-cloud environments and ensure seamless integration with existing systems while navigating evolving legal frameworks.

Looking forward, future developments are expected to include hybrid cloud architectures, edge computing for low-latency processing, and potential integration with blockchain technologies to further strengthen security and transparency. These innovations will continue to drive the digital transformation of the financial sector,

helping organizations improve operational efficiency, enhance customer trust, and sustain competitive advantage.

Internet of Things

IoT can play an important role in the financial sector by enabling real-time data collection and monitoring. It can improve customer experiences through instant alerts and biometric authentication, optimize loan management by tracking borrower behavior and collateral, and automate payments via machine-to-machine communication. However, its adoption is limited due to significant security and privacy concerns leading to a slower implementation. Interconnected devices can also increase the risk of cyberattacks and data breaches, requiring investment in strong encryption and continuous monitoring.

Quantum Computing

Quantum computing is recognized as having a great potential in the financial sector, but its current application remains very limited. Although financial institutions are increasingly aware of quantum computing's capabilities, the technology has yet to be widely adopted due to high costs and the lack of clear and immediate benefits. Still, financial institutions are closely monitoring the implications of quantum computing on financial security, since quantum machines could potentially break existing encryption methods, necessitating new quantum-resistant cryptography protocols.

Neurocomputing

Even though there are indications of interest in the general use of neurocomputing in the financial sector, its applications are currently mostly related to research.

Application Programming Interface

APIs are among the most widely used technologies in the financial sector. They primarily connect on-premise systems with cloud infrastructure, enabling integration across different platforms. APIs are crucial to open banking, allowing secure data to be shared between financial institutions and third-party providers. However, APIs can

introduce security risks such as data breaches, unauthorized access, and DDoS attacks, if it has weak authentication and non-reliable third-party providers.

Robotic Process Automation

RPA is primarily used to automate repetitive processes, such as reading digital documents and scanning physical documents to convert them into digital formats. Originally focused on simple rule-based tasks, RPA has evolved to allow the usage of AI and ML, enabling it to handle more complex activities and support decision-making processes.

Question 2: How will emerging technologies influence the financial sector in the short and medium term?

It is a difficult task to know the possible evolution of technology. Yet, the technology we know today should evolve in such a way that in the next 5 to 10 years, the way we do business and the way we, as investors, customers, policyholders, and institutions interact with technology should change in an entirely new form.

Artificial Intelligence

AI is anticipated to become one of the most transformative technologies in the financial sector over the short to medium term, with continued improvements expected in both capability and adoption. Initially, firms are concentrating AI efforts on back-office operations to enhance efficiency and reduce manual processes. However, as AI matures, its application is expected to broaden significantly, impacting client interactions by improving personalization, speeding up service delivery, and increasing the quality of customer support. AI's growing role in fraud detection and risk assessment will also strengthen financial institutions' ability to manage risks more effectively. Also, while it has been stated that financial institutions currently avoid the use of generative AI in their core business operations, the broader trend suggests this may change in the near future. As generative AI technologies mature and institutions gain more familiarity and confidence in their capabilities, their use is expected to expand to continue improving

internal operations and customer interactions, particularly through automation and data analysis.

AI is likely to reshape the structure of financial services by reducing the number of intermediaries, thereby providing customers with more direct and streamlined access to financial products. While this can enhance process speed and reduce costs, it also raises concerns about the potential loss of human touch in customer interactions, which could affect client trust and satisfaction if not carefully managed.

Furthermore, AI-driven personalization will demand greater acquisition and processing of sensitive personal data, raising critical issues around data privacy and cybersecurity. Institutions will need to invest substantially in safeguarding data assets and ensuring compliance with evolving regulations. These challenges highlight the importance of balancing innovation with ethical and security considerations as AI adoption accelerates.

Overall, while the current focus remains on operational improvements, there is a possibility that the medium-term impact of AI will be broader and more profound, touching on customer experience, risk management, and the overall business model of financial institutions. This evolution will require not only technological upgrades but also strategic workforce planning and policy adjustments to fully realize AI's potential benefits and mitigate associated risks.

The effectiveness of AI and ML technologies relies heavily on the quality of data, as poor or noisy data can undermine AI performance and lead to inaccurate outcomes. As such, it's expected for organizations to focus on improving data collection, cleaning, and validation, to benefit from more reliable AI solutions.

Human management is going to be vital for efficient AI control systems. The integration of human supervisors within AI workflows will improve accuracy and safety by allowing intervention in uncertain or high-risk situations. It's to be expected that most institutions in the future will have AI to support human decisions rather than fully replacing them. However, if some institution falls under the belief that AI can fully automate and replace the human role, there also exists the possibility of the reduction of workforces, increasing the number of layoffs.

Additionally, the demand for AI-related skills is expected to continue to grow. Not only skills completely related to AI roles such as data scientists, but also more general

knowledge for employees to be able tp engage with AI as a tool embedded in their work. This can lead to institutions requiring employees to learn new skills in collaboration and interpretation of AI outputs. As such, companies should start investing in AI education and training, so as to be better positioned to adapt and utilize these technologies effectively.

The expected increasing adoption and evolution of AI in the financial sector is likely to also bring notable risks. One of the main concerns is the potential for biases within AI models, which, if not properly managed, could lead to unfair or inaccurate decision-making. The widespread use of similar AI systems across institutions also raises the risk of systemic vulnerabilities. During periods of market stress, these shared dependencies might amplify financial instability, as many entities rely on comparable algorithms and data inputs.

Moreover, many AI systems lack transparency, creating challenges for regulatory oversight and risk management. This opacity underscores the urgent need for robust frameworks that support thorough testing, validation, and explainability of AI models. Such frameworks are essential to ensure compliance, reduce operational risks, and maintain trust among stakeholders in a landscape that is becoming increasingly automated.

These risks are aggravated by some workforce challenges, including current gaps in AI expertise and uneven adoption across different financial sectors. Consumer skepticism and concerns over data privacy and cybersecurity are some other expected concerns. Additionally, the possibility of issues like algorithmic bias and model "hallucinations" to be able to distort market outcomes can complicate risk management and decision-making. Some of the biggest changes yet to be discovered should be related to addressing these challenges, so as to have the benefits of AI while minimizing its potential downsides.

Blockchain

Emerging technologies such as blockchain are expected to play an increasingly significant role in the financial sector, particularly in capital markets and payment systems. The adoption of blockchain technology is likely to enhance efficiency by reducing the reliance on intermediaries, which can simplify transactions and lower costs. This evolution may contribute to greater financial inclusion by enabling more accessible and

affordable financial services for underserved populations, leading to a possible broader adoption of this technology.

However, the growing use of blockchain and related technologies will also bring some challenges, particularly in the areas of data privacy and cybersecurity. As financial institutions collect and process larger volumes of sensitive data, concerns over confidentiality and the potential for cyberattacks will become more prominent. Ensuring the secure management of cryptographic keys and addressing vulnerabilities in distributed networks will be important to maintaining trust in these systems.

Current research suggests that blockchain has the potential to integrate more deeply into traditional financial infrastructures, including clearinghouses, securities depositories, and trading platforms. This integration could lead to more transparent, secure, and efficient systems, but it will require overcoming technical and regulatory challenges, such as interoperability between systems and compliance with data protection regulations.

Cloud Computing

Emerging technologies, particularly AI and Big Data, are intensifying the demand for cloud computing services within the financial sector. This increased reliance on cloud infrastructures is likely to lead to broader adoption and expansion of cloud computing in both the short and medium term. Cloud computing acts as an important enabler, serving as a "bridge" that connects various emerging technologies, allowing for more scalable, agile, and cost-effective operations.

Despite historical hesitation due to regulatory constraints and legacy system complexities, more recently financial institutions have increasingly embraced cloud solutions, leading to a high possibility of continuing to increase its adoption in the following years. Recent regulatory adjustments and a better understanding of cloud benefits, such as operational agility and cost efficiency, are some of the main reasons for this expectation.

Cloud computing infrastructure is expected to continue its rapid growth and global expansion in the coming years. Leading providers will likely continue to enhance bandwidth and strengthen disaster recovery capabilities to meet evolving financial sector needs. It is projected for cloud resources to be even closer to data sources, further

improving performance and connectivity. While cloud services are not yet uniformly accessible worldwide, ongoing investments in infrastructure will likely broaden availability, especially in emerging markets, supporting the sector's increasing reliance on cloud technologies.

Financial sector cloud adoption is part of a larger trend poised for substantial growth. While revenue growth rates have currently slightly decelerated, cloud providers continue to generate significant income, with projections estimating the market could reach around $1 trillion by 2030. This trajectory suggests cloud computing is in an early expansion phase, with potential to replace traditional on-premise systems in the following years.

Internet of Things

IoT may hold the potential to enable real-time data exchange, automation, enhance security, and improve customer service. These capabilities could support areas such as loan management, collateral monitoring, personalized banking, automated payment systems, and customer relations. However, alongside these opportunities, IoT may also introduce some challenges, which, if not well managed, can lead to data security concerns, cyber threats, and lack of regulatory compliance. The expectations for IoT in the financial sector are mixed, even though it can bring promising impacts, it can also bring the development of bigger concerns of privacy and security leading adoption and evolution challenges. As such, some believe that IoT will see more applications in the future, while some might also consider that institutions may lack the necessary caution or that the associated risks are too high for a broader implementation.

Quantum Computing

Emerging quantum computing technologies hold the potential to influence financial institutions, particularly in areas like risk assessment. While some experts foresee significant roles for quantum computing within the next five to ten years, skepticism remains due to high costs and current technological limitations. The pace of advancement depends not only on increasing qubit numbers but also on improvements in algorithms, error correction, and hardware reliability, with practical applications more likely emerging around 2035 or later.

A major concern related to quantum computing involves its impact on cryptography. Quantum machines could potentially break existing encryption methods that secure digital communications and transactions, posing a threat to the confidentiality and integrity of financial data. Another possible challenge is dealing with "store-and-break" threats, meaning that adversaries might intercept sensitive data now and decrypt it in the future once quantum capabilities have matured. Consequently, there is a pressing need and expectation for financial institutions to adopt quantum-resistant encryption methods proactively, rather than waiting for formal standards to be established. Ultimately, the responsibility for securing financial systems against quantum threats will require coordinated efforts from developers, institutions, and users to deal with sensitive information and maintain trust as quantum computing evolves.

Neurocomputing

Neurocomputing is an emerging technology that mayt hold promise for the financial sector, but it is still too early in its development stages to be known. Current advancements, such as Intel's neuromorphic research chip designed to mimic brain architecture, indicate progress in this field. However, given the infancy of neurocomputing technology, its practical applications and impact within the financial sector remain uncertain and difficult to predict at this time. It is not expected to become widely available or influential in the near future, likely requiring a decade or more before a more significant appearance occurs.

Application Programming Interface

APIs will remain an essential technology in the financial sector, particularly in enabling open banking and secure data exchange between institutions and third-party providers. Although there is a perception that API technology may have reached maturity, emerging regulatory changes such as the upcoming PSD3 are expected to create significant enhancements, especially in security.

Current challenges with APIs include risks like data breaches and unauthorized access, often stemming from weak authentication and vulnerabilities in third-party providers. Financial institutions must therefore implement better security measures, including strong

authentication protocols, API gateways, traffic monitoring, and look for rigorous partners so as to maintain system integrity.

PSD3 is expected to introduce stricter functional requirements and transparency obligations that aim to encourage trust and usability in open banking APIs. By mandating user-accessible monitoring and improved security standards, PSD3 not only is expected to enhance consumer protection but also level the playing field among payment service providers.

As such, while API technology itself may seem stable, evolving regulations and security demands ensure that APIs will continue to develop, particularly in ways that support safer, more transparent, and resilient financial operations.

Robotic Process Automation

OCR currently plays a complementary role in the development and improvement of RPA's ability to extract and process information from unstructured sources such as scanned documents or handwritten forms. Advances in deep learning and natural language processing are expected to make OCR more accurate and context-aware, thereby extending the range of processes that RPA can handle without human intervention.

Looking at the evolution of RPA—from basic rule-based automation to systems capable of mimicking human judgment—there is a clear trajectory toward increasingly intelligent automation. While current systems still rely on human oversight for high-risk or ambiguous tasks, continued improvements in supporting technologies like OCR suggest that RPA will become even more autonomous and adaptable, potentially reshaping workflows within financial institutions.

Question 3: What are the potential regulatory challenges created by the expected evolution of emerging technologies in the financial sector?

Currently, regulators tend to wait until a technology reaches a certain scale or risk level before intervening, likely in an effort to avoid overregulation or misjudging its true impact. However, this reactive attitude may prove problematic in a future where technological innovation occurs at never experienced speed and scale. As a result, regulators may struggle to keep pace with more complex evolutions of technologies, such

as AI. These innovations, if left unregulated or loosely regulated, could lead to an increase in systemic risk, especially when they become more integrated in the core operations of institutions in the financial sector. The inability to anticipate and manage such risks may also in turn lead to financial instability, particularly if the regulatory response remains fragmented or outdated.

As financial technologies evolve, existing legal definitions and frameworks risk becoming obsolete or misaligned with market realities. This could either suppress innovation through excessive constraints or leave dangerous gaps where prejudicial practices can occur. Although the EU has taken steps through initiatives like MiCA, DORA, and the DLT Pilot Regime, regulatory fragmentation across jurisdictions remains a challenge. The uneven adoption of these frameworks outside the EU may create opportunities to exploit regulatory loopholes, allowing firms to take advantage of more lenient legal environments. As such, coordinating regulatory approaches internationally will be increasingly difficult, especially for technologies like DeFi or Cloud Computing, which easily defy geographical barriers. At the same time, the possibility of overregulation could harm the development and deployment of new financial technologies, while under regulation might expose consumers and institutions to cyber threats, fraud, and systemic failures. A more flexible regulatory approach to regulation and experimentation through sandboxes may lead to a better adaptability but knowing when to move from testing to full implementation, and how to monitor ongoing impacts in real-time, will possibly remain a difficult task. The growing digitalization of processes in the financial sector can also bring more cybersecurity risks. Technologies like AI can help strengthen security but can also become another target for exploits. As anticipated in DORA, future regulatory regimes will possibly need to continuously evolve to address these threats without overburdening smaller institutions that may lack the capacity for full compliance. In Data governance, while data-driven innovation depends on broad access to high-quality information, an increase in strict privacy regulations may introduce bureaucratic obstacles and reduce the availability of usable data. This could also lead to an increase in regulatory challenges, elevated costs, and impaired innovation.

Finally, ensuring that regulatory institutions are equipped to address these challenges will require significant investment, especially in cybersecurity. Institutions must adopt advanced analytical tools and simulation models to detect risks and design corresponding responses. Yet, many public regulatory institutions may face difficulties attracting and

retaining experts with the technical knowledge required to understand and regulate sophisticated financial technologies, especially since the private sector usually offers more lucrative and better opportunities. This can create a risk of weakening the capability and effectiveness of regulators to precisely react to the risks of technological transformation.

6. Conclusion

The financial sector may expect significant transformations in the application of emerging technologies, which are set to reshape how institutions will operate and interact with their clients in future. Technologies such as AI, blockchain, cloud computing, IoT, quantum computing, API, and RPA promise to enhance efficiency, improve personalization, increase security, and enable new business models. These technologies may have the potential to reduce costs, simplify processes, and increase financial inclusion, while also creating new unforeseen opportunities. However, this technological evolution also introduces considerable challenges. Financial institutions must address issues such as, but not limited to, data privacy, cybersecurity, algorithmic bias, workforce adaptation, and system interoperability. The increasing reliance on technology may increase the difficulty of managing operational risks and maintaining trust in financial markets. Alongside these operational and strategic changes, regulations are expected to evolve so as to keep pace with technological innovation. Traditional regulatory approaches, often reactive and fragmented, may struggle to effectively manage complex new technologies without impairing innovation. Regulators may face the difficult task of balancing risk management with raising a supportive environment for experimentation and growth. Enhanced coordination, flexible frameworks such as regulatory sandboxes, and investment in regulatory expertise are essential to managing systemic risks and protecting consumers. Still, while emerging technologies may offer transformative potential and challenges that can revolutionize the financial sector, their successful adoption and evolution will depend a lot on the decision of the financial institutions and authorities.

To further improve this study, it would be necessary to conduct additional interviews, to improve their scripts, and study additional more in-depth literature. This would allow for more detailed and richer conversations, as some of the interviews conducted for this thesis were limited in scope due to time constraints. Expanding the literature review to include the latest research and case studies would also provide even stronger foundations, findings, and points of view. Furthermore, given the fast expected pace evolution of technology, it is essential to continuously update the information and redo the study so as to reflect new developments, innovations, and regulatory changes.

References

Agrawal, R., Desai, S., Dholwani, D., Kedari, N. and Banerjee, A. (2024). Artificial Intelligence/Machine Learning Driven Decision making in Business Analytics for Financial Sector using Ensemble Machine Learning Techniques. pp.371–376. doi:https://doi.org/10.1109/aic61668.2024.10731028.

Ahern, D. (2021). Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers: Calibrating an EU Response to the Regulatory Sandbox Phenomenon. *European Business Organization Law Review*, 22(1), pp.395–432. doi:https://doi.org/10.1007/s40804-021-00217-z.

Ahern, D. (2025). The New Anticipatory Governance Culture for Innovation: Regulatory Foresight, Regulatory Experimentation and Regulatory Learning. *European Business Organization Law Review*, 6(1). doi:https://doi.org/10.48550/arXiv.2501.05921.

Akoh, A., Ike, C., Franca, O., Samson, B., Ndubuisi, L. and Adura, R. (2024). THE INTERSECTION OF AI AND QUANTUM COMPUTING IN FINANCIAL MARKETS: A CRITICAL REVIEW. *Computer science & IT research journal*, 5(2), pp.461–472. doi:https://doi.org/10.51594/csitrj.v5i2.816.

Banco de Portugal (n.d.). *Institutions | Portal do Cliente Bancario*. [online] Bportugal.pt. Available at: https://clientebancario.bportugal.pt/en/institutions.

Bank of England (2025). *Financial Stability in Focus: Artificial intelligence in the financial system*. [online] Bank of England. Available at: https://www.bankofengland.co.uk/financial-stability-in-focus/2025/april-2025.

Beau, D. (2024). *Emerging Technologies in Financial Services: Opportunities and Challenges | Autorité de contrôle prudentiel et de résolution*. [online] Autorité de contrôle prudentiel et de résolution. Available at: https://acpr.banque-france.fr/fr/interventions-gouverneur/emerging-technologies-financial-services-opportunities-and-challenges.

Central Bank of Ireland (n.d.-a). *What is financial regulation and why does it matter?* [online] Central Bank of Ireland. Available at: https://www.centralbank.ie/consumer-hub/explainers/what-is-financial-regulation-and-why-does-it-matter.

Central Bank of Ireland (n.d.-b). *What Is 'fintech' and How Is It Changing Financial products?* [online] Central Bank of Ireland. Available at: https://www.centralbank.ie/consumer-hub/explainers/what-is-fintech-and-how-is-it-changing-financial-products.

Chapman, D., Zaal, S. and Kernahan, R. (2024). *Transforming financial services with cloud and AI*. [online] Capgemini. Available at: https://www.capgemini.com/insights/expert-perspectives/the-cloud-and-ai-race-in-financial-services/.

Choi, D. and Lee, K. (2018). An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation. *Security and Communication Networks*, [online] 2018(5483472), pp.1–15. doi:https://doi.org/10.1155/2018/5483472.

Deloitte (n.d.). *Quantum computing: Unlocking the unknown | Deloitte Luxembourg*. [online] Deloitte. Available at: https://www.deloitte.com/lu/en/Industries/technology/blogs/quantum-computing.html.

Deloitte (2018-a). *Blockchain Legal implications, questions, opportunities and risks*. [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/sv/Documents/legal/Blockchain%20WP%20March%202018_.pdf.

Deloitte (2018-b). *What is cloud computing? | Technology | Deloitte Digital + Salesforce*. [online] Deloitte. Available at: https://www.deloitte.com/mt/en/Industries/technology/perspectives/mt-salesforce-what-is-cloud-computing.html.

Deloitte (2021). *What is IoT?* [online] Deloitte. Available at: https://www.deloitte.com/ch/en/services/consulting/perspectives/iot-explained.html.

Deloitte (2024). Financial Services: Prepare for a Regulatory Refresh. *Risk & Compliance Journal*. [online] Available at: https://deloitte.wsj.com/riskandcompliance/financial-services-prepare-for-a-regulatory-refresh-284370ba.

Ekiye, A.E. and Hewage, P. (2024). Comparative Analysis of Machine and Deep Learning Techniques for Credit Card Fraud Prediction in The Financial Sector. *2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0*, pp.1–6. doi:https://doi.org/10.1109/otcon60325.2024.10688293.

EUR-Lex (2024). *Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 Text with EEA relevance*. [online] Available at: http://data.europa.eu/eli/reg/2013/575/2024-07-09.

European Central Bank (n.d.). *Insurance corporationn statistics*. [online] European Central Bank. Available at: https://www.ecb.europa.eu/stats/financial_corporations/insurance_corporations/html/index.en.html.

European Union (n.d.) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, AI Act, Article 26. Available at at: https://ai-act-law.eu/article/26/.

Federal Reserve Bank of St. Louis (2017). *Capital Markets - Stock Market Game, Ep. 1*. [online] YouTube. Available at: https://www.youtube.com/watch?v=n7st0D0HUAQ.

Fong, D., Han, F., Liu, L., Qu, J. and Shek, A. (2021). *Seven technologies shaping the future of fintech | McKinsey*. [online] McKinsey & Company. Available at: https://www.mckinsey.com/cn/our-insights/our-insights/seven-technologies-shaping-the-future-of-fintech.

Fridman, L., Ding, L., Jenik, B. and Reimer, B. (2017). Arguing Machines: Human Supervision of Black Box AI Systems That Make Life-Critical Decisions. arXiv. doi:https://doi.org/10.48550/arXiv.1710.04459.

Galhardo-Burnett, J., Engelhardt, M., Ramachandran, S., Santhanam, P. and Scognamiglio, F. (2023). *Cloud Cover: Introducing a Standardized Pricing Index*. [online] Boston Consulting Group. Available at:

https://www.bcg.com/publications/2023/the-four-trends-shaping-the-cloud-industry.

Globe Newswire (2025). *FinTech Blockchain Global Industry Report 2025: Decentralized Finance (DeFi) to Bridge the Huge SME Financing Gap to Boost Blockchain Adoption*. [online] Fintech Futures. Available at: https://www.fintechfutures.com/press-releases/fintech-blockchain-global-industry-report-2025-decentralized-finance-defi-to-bridge-the-huge-sme-financing-gap-to-boost-blockchain-adoption.

Green, A. (2024). *Artificial intelligence and the changing demand for skills in the labour market*. [online] OECD. Available at: https://www.oecd.org/en/publications/artificial-intelligence-and-the-changing-demand-for-skills-in-the-labour-market_88684e36-en.html.

Groenland, K. (2025). *The timelines: when can we expect useful quantum computers?* [online] Introduction to Quantum Computing for Business. Available at: https://introtoquantum.org/essentials/timelines/#putting-it-all-together.

Zee, H. H. (2004). *Taxing the Financial Sector*. *International Monetary Fund eBooks*, 700 19th Street, N.W., Washington, D.C. 20431, U.S.A: International Monetary Fund, pp.16–31. doi:https://doi.org/10.5089/9781589063167.071.

Haro-Olmo, F.J. de, Varela-Vaca, Á.J. and Álvarez-Bermejo, J.A. (2020). Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review. *Sensors*, 20(24). doi:https://doi.org/10.3390/s20247171.

Hossain, M.A., Raza, Md.A. and Rahman, J.Y. (2025). Investigating the Cybersecurity Implications of Open Banking and Application Programming Interfaces (APIs) in the Financial Sector. *Ministal*, 4(1), pp.39–56. doi:https://doi.org/10.55927/ministal.v4i1.13370.

Intel (2021). *Intel Advances Neuromorphic with Loihi 2, New Lava Software Framework and New Partners*. [online] Intel Corporation. Available at: https://www.intc.com/news-events/press-releases/detail/1502/intel-advances-neuromorphic-with-loihi-2-new-lava-software.

International Finance Corporation (n.d.). *Capital Markets*. [online] IFC. Available at: https://www.ifc.org/en/what-we-do/sector-expertise/financial-institutions/capital-markets.

Jain, R. (2023). Role of artificial intelligence in banking and finance. *Journal of Management and Science*, 13(3), pp.1–4. doi:https://doi.org/10.26524/jms.13.27.

Johri, S., Singh, S.K., Reddy, C.V., Nijhawan, G., Alawadi, A.H. and Reddy, U. (2023). Improving Security and Effectiveness in Banking Operations with IoT Integration. *2024 IEEE International Conference on Contemporary Computing and Communications (InC4)*. doi:https://doi.org/10.1109/upcon59197.2023.10434723

J.P. Morgan (2024). *PSD3: The EU's Third Payment Services Directive | J.P. Morgan*. [online] J.P. Morgan. Available at: https://www.jpmorgan.com/insights/payments/payments-optimization/psd3.

Khang, A. (2025). *Shaping Cutting-Edge Technologies and Applications for Digital Banking and Financial Services*. [online] Google Books. Available at: https://books.google.pt/books?hl=pt-PT&lr=&id=Cjw_EQAAQBAJ&oi=fnd&pg=PA106&dq=implementation+of+quantum+computing+in+financial+sector&ots=hY1wBuYrYU&sig=i08scj866r2Fs8VHN3JR8saWJJs&redir_esc=y#v=onepage&q=implementation%20of%20quantum%20computing%20in%20financial%20sector&f=false.

Kour, M. (2024). Revolutionizing Finance: Unleashing Machine Learning's Potential for a New Financial Era. 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET), pp.1–5. doi:https://doi.org/10.1109/acroset62108.2024.10743732.

Leitner, G., Singh, J., Kraaij, A. van der and Zsámboki, B. (2024). The rise of artificial intelligence: benefits and risks for financial stability. *Financial Stability Review, May 2024*. [online] Available at: https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html.

Manikandan, M., Venkatesh, P., Chitra, D., Krishnamoorthi, M., Ramu, M. and Senthilnathan, C.R. (2024). An Impact of Artificial Intelligence in Fintech. pp.1–3. doi:https://doi.org/10.1109/icpects62210.2024.10780020.

Marr, B. (2024). The 10 Most Important Banking And Financial Technology Trends That Will Shape 2025. *Forbes*. [online] 13 Nov. Available at: https://www.forbes.com/sites/bernardmarr/2024/11/13/the-10-most-important-banking-and-financial-technology-trends-that-will-shape-2025/.

Mayer, H., Yee, L., Chui, M. and Roberts, R. (2025). *Superagency in the workplace: Empowering people to unlock AI's full potential*. [online] McKinsey & Company. Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work.

Misra, S.C. and Doneria, K. (2018). Application of cloud computing in financial services: an agent-oriented modelling approach. *Journal of Modelling in Management*, 13(4), pp.994–1006. doi:https://doi.org/10.1108/jm2-12-2017-0131.

Moscetti, L. and Bali, A. (2025). *AI Adoption in European Financial Services: Progress, Challenges, and Future Directions*. [online] EY. Available at: https://www.ey.com/en_lu/insights/ai/ai-adoption-in-european-financial-services-progress-challenges-and-future-directions.

Narayana, L. and Panigrahi, S. (2024). Novel Methodology of Adaptive Machine Learning and Deep Learning System for Detecting the Fraudulent Activities in Financial Sector. *2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0*, [online] pp.1–6. doi:https://doi.org/10.1109/inc460750.2024.10649371.

Panduro-Ramirez, J., Sharma, A.K., Singh, G., Pavana, K.H., Poma-Garcia, C. and Shukla, S.K. (2022). Blockchain Implementation in Financial Sector and Cyber Security System. *2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)*, pp.754–760. doi:https://doi.org/10.1109/smart55829.2022.10047779.

Pandy, G., Jayaram, V., Krishnappa, M.S., Ingole, B.S., Ganeeb, K.K. and Joseph, S. (2024). Advancements in Robotics Process Automation: A Novel Model with Enhanced Empirical Validation and Theoretical Insights. *European Journal of Computer Science and Information Technology*, 12(5), pp.64–73. doi:https://doi.org/10.37745/ejcsit.2013/vol12n56473.

PricewaterhouseCoopers (n.d.). *Blockchain's impact in fostering global financial inclusion*. [online] PwC. Available at: https://www.pwc.com/us/en/services/digital-assets/blockchain-financial-inclusion.html.

PYMNTS (2024). *72% of Finance Leaders Use AI in Their Operations | PYMNTS.com*. [online] PYMNTS. Available at: https://www.pymnts.com/artificial-intelligence-2/2024/72percent-of-finance-leaders-use-ai-in-their-operations/.

Rajput, H. and Saxena, K. (2023). Utilizing IoT-Based Services to Reduce Financial Risks in the Banking Sector. *2023 1st International Conference on Circuits, Power and Intelligent Systems (CCPIS)*, pp.01–06. doi:https://doi.org/10.1109/ccpis59145.2023.10291931.

Sarda, P., Chowdhury, M.J.M., Colman, A., Kabir, M.A. and Han, J. (2018). *Blockchain for Fraud Prevention: A Work-History Fraud Prevention System*. IEEE Xplore. doi:https://doi.org/10.1109/TrustCom/BigDataSE.2018.00281.

Schatsky, D., Muraskin, C. and Gurumurthy, R. (2014). *A Deloitte series on cognitive technologies Demystifying artificial intelligence What business leaders need to know about cognitive technologies*. [online] Available at: https://pt.scribd.com/document/358283277/Demystifying-Artificial-Intelligence-pdf.

Scholl, M. (2021). *Post-Quantum Cryptography: A Q&A With NIST's Matt Scholl*. [online] NIST. Available at: https://www.nist.gov/blogs/taking-measure/post-quantum-cryptography-qa-nists-matt-scholl.

Schuman, C.D., Potok, T.E., Patton, R.M., Birdwell, J.D., Dean, M.E., Rose, G.S. and Plank, J.S. (2017). A Survey of Neuromorphic Computing and Neural Networks in Hardware. *arXiv*. doi:https://doi.org/10.48550/arXiv.1705.06963.

Shekhar, S. (2025). UNLOCKING THE POWER OF AI OPTICAL CHARACTER RECOGNITION FOR REAL-TIME DATA PROCESSING. *ResearchGate*. Available at: https://www.researchgate.net/publication/387723122_UNLOCKING_THE_POWER_OF_AI_OPTICAL_CHARACTER_RECOGNITION_FOR_REAL-TIME_DATA_PROCESSING.

Suseendran, G., Chandrasekaran, E., Akila, D. and Sasi Kumar, A. (2019). Banking and FinTech (Financial Technology) Embraced with IoT Device. *Data Management, Analytics and Innovation*, 1, pp.197–211. doi:https://doi.org/10.1007/978-981-32-9949-8_15.

Tang, C.-P., Huang, T.C.-K. and Wang, S.-T. (2018). The impact of Internet of things implementation on firm performance. *Telematics and Informatics*, 35(7), pp.2038–2053. doi:https://doi.org/10.1016/j.tele.2018.07.007.

Tartaro, A., Smith, A.L. and Shaw, P. (2023). Assessing the impact of regulations and standards on innovation in the field of AI. arXiv. doi:https://doi.org/10.48550/arXiv.2302.04110.

Taylor, C., Wilson, C.D., Holttinen, E. and Morozova, A. (2020). Institutional Arrangements for Fintech Regulation and Supervision. *FinTech Notes*, 2019(002). doi:https://doi.org/10.5089/9781513520308.063.

Thirumagal, P.G., Das, T., Das, S., Khatri, E., S., K. and Rani, S. (2024). The Role of IoT in Revolutionizing Payment Systems and Digital Transactions in Finance. *2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)*. doi:https://doi.org/10.1109/icrtcst61793.2024.10578351.

Thompsett, L. (2025). *Top 10: Emerging Technologies in Finance*. [online] Fintechmagazine.com. Available at: https://fintechmagazine.com/articles/top-10-emerging-technologies-in-finance.

Vadisetty, R. (2024). Efficient Large-Scale Data based on Cloud Framework using Critical Influences on Financial Landscape. *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)*, pp.1–6. doi:https://doi.org/10.1109/icec59683.2024.10837096.

Vukovljak, B. (2023). Blockchain as an Instrument for Improving Banking Processes. *Naše Gospodarstvo*, 69(1), pp.43–55. doi:https://doi.org/10.2478/ngoe-2023-0005.

Whang, S.E., Roh, Y., Song, H. and Lee, J.-G. (2023). Data Collection and Quality Challenges in Deep Learning: A Data-centric AI Perspective. *The VLDB Journal*, 32(2), pp.791–813. doi:https://doi.org/10.1007/s00778-022-00775-9.

World Bank (n.d.-a). *Financial Development*. [online] World Bank. Available at: https://www.worldbank.org/en/publication/gfdr/gfdr-2016/background/financial-development.

World Bank (n.d.-b). *Nonbanking Financial Institution*. [online] World Bank. Available at: https://www.worldbank.org/en/publication/gfdr/gfdr-2016/background/nonbank-financial-institution.

Yahiya, A., Kumari, S.S., S, M., Guha, S.K., Gehlot, A. and Pant, B. (2023). Blockchain Implementation in Financial Sector and Cyber Security System. *2024 IEEE International Conference on Contemporary Computing and Communications (InC4)*. doi:https://doi.org/10.1109/aisc56616.2023.10085045.

Zhang, B., Rowan, P., Duff, S., Homer, M., Schizas, E., Soriano, M., Cloud, K., Umer, Z., Garvey, K., Ziegler, T., Wardrop, R., Alam, N., Blandin, A., Gray, M., Chen, H.-Y., Johanson, D., Yerolemou, N., Anil, K., Calabia, C. and Chantramonklasri, T. (2019). *Early Lessons on Regulatory Innovation to Enable Inclusive FinTech*. [online] *Cambridge Centre for Alternative Finance*. Cambridge, United Kingdom: Cambridge Centre for Alternative Finance. Available at: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/early-lessons-on-regulatory-innovation-to-enable-inclusive-fintech/.

Литвин, О., Кудін, В., Онищенко, А., Ніколаєв, М. and Чаплинська, Н. (2024). INTEGRATION OF DIGITAL MEANS IN THE FINANCIAL SPHERE: THE POTENTIAL OF CLOUD COMPUTING, BLOCKCHAIN, BIG DATA AND AI. *Financial and credit activity problems of theory and practice*, 1(54), pp.127–145. doi:https://doi.org/10.55643/fcaptp.1.54.2024.4257.