






## Assessing the impact of financial technology: Is it a curse or blessing for financial crimes in financial institutions?

 **Tipon Tanchangya**<sup>1+</sup>

 **Kamron Naher**<sup>2</sup>

 **Md Rakib Mia**<sup>3</sup>

 **Srima Chowdhury**<sup>4</sup>

 **Naimul Islam**<sup>5</sup>

<sup>1</sup>Department of Finance, University of Chittagong, Chittagong 4331, Bangladesh.

Email: [tipon.tcg.edu@gmail.com](mailto:tipon.tcg.edu@gmail.com)

<sup>2</sup>Department of Business, Presidency University, Dhaka-1212, Bangladesh.

Email: [naherk@pu.edu.bd](mailto:naherk@pu.edu.bd)

<sup>3</sup>Department of Business Administration, Ahsanullah University of Science and Technology, Dhaka, Bangladesh.

Email: [mdrakibmia087@gmail.com](mailto:mdrakibmia087@gmail.com)

<sup>4</sup>Department of Accounting, University of Chittagong, Chittagong 4203, Bangladesh.

Email: [srrimachy@gmail.com](mailto:srrimachy@gmail.com)

<sup>5</sup>Department of Accounting, Finance and Economics, University of Greenwich, London SE10 9LS, UK.

Email: [naimmgtdu75@gmail.com](mailto:naimmgtdu75@gmail.com)



(+ Corresponding author)

### ABSTRACT

#### Article History

Received: 30 September 2024

Revised: 14 January 2025

Accepted: 24 January 2024

Published: 31 January 2025

#### Keywords

Blessing of financial technologies

Curse of financial technologies

Financial crimes

Financial institutions

Financial technologies.

Cybercrimes

The study aims to assess the dual (positive and negative) impact of FinTech in financial institutions. In this study, secondary data were used, and they were collected from Web of Science, Scopus, ScienceDirect, and Google Scholar. In this regard, the key FinTech technologies are identified, including blockchain and distributed ledger technology, artificial intelligence and machine learning, robo-advisors, mobile banking and digital banking, regulatory technology, and cloud computing. While major financial crimes are fraud, money laundering, insider trading, bribery and corruption, tax evasion, and cybercrime, The study shows that AI algorithms help to identify criminal activities, including credit card fraud, theft, and account takeovers, and ensure data privacy, accountability, and transparency. Blockchain is useful for trustless transactions since it creates an unchangeable and secure, transparent record of every transaction. Big data analytics help to acquire insights into customer behaviour and preferences. RegTech tracks online transactions in real time to spot anomalies in the realm of digital payments. On the other hand, FinTech is one of the most effective tools to facilitate cybercrime. Moreover, the study shows the framework FinTech has for mitigating wrongdoing, regulatory shortages, and customer threats. The article provides several implications for several stakeholders in the financial sector.

**Contribution/Originality:** This study has significant contributions for the financial institutions. Financial technologies are basically invented to work for the financial development all over the world. Financial institutions should invest in a cybersecurity system to protect all information from cyberattacks. The government must ensure the security of the financial institutions.

### 1. INTRODUCTION

The financial crisis in 2008 had a significant influence on the emergence of financial technology (FinTech), which was positively affected by the emergence of cryptocurrencies like Bitcoin in 2009. The objective behind the implementation of FinTech is to improve the financial performance of the organisation through digitalisation (Schueffel, 2016). The growth of the industry is identified by the value of investment, which is enhanced by 75% in 2015 compared to the previous year, and furthermore, since 2010, approximately USD 50 billion has been invested

(Skan, Dickerson, & Gagliardi, 2016). FinTech provides financial services more efficiently than traditional banking services by focusing on big data, efficient risk and maturity transformation, decentralised access to data, etc. (Navaretti, Calzolari, Mansilla-Fernandez, & Pozzolo, 2018). However, the emergence of FinTech magnifies the competition of traditional banking as new competitors (such as startups, neobanks, etc.) are entering the financial industry, which enhances the quality of services like remittance, payments, crowdfunding, and so on (Murinde, Rizopoulos, & Zachariadis, 2022).

The growth of financial crime is increasing dramatically. Numerous notable regulations are introduced to minimise financial crime, including the Foreign Corrupt Practices Act, 1977, by the U.S. and the Bribery Act, 2010. According to Rybalchenko, Ryzhkov, and Ohrimenco (2021) the main motive behind the financial or economic crime is economic gain through money laundering, tax evasion, investment fraud, etc. In the technological era, crime increases with the usage of hacking tools and engineering techniques (Hasham, Joshi, & Mikkelsen, 2019). Hence, the term “financial cybercrime” has been introduced in different studies by researchers, which consists of illegal economic activities for obtaining financial gain in cyberspace (Nicholls, Kuppa, & Le-Khac, 2021). In addition, the Advertising Standard Authority and Committee of Advertising reveal a 190% increase in losses from cryptocurrency scams (Trozze et al., 2022). The reason behind the global financial crisis is the weakness of the corporate governance architecture of the FinTech firms, and therefore, a new infrastructural corporate governance that meets the FinTech phenomenon will reduce the global financial crisis by developing an effective global financial system (Alade, 2023).

In the financial field, FinTech is recognised as the most advanced innovation for enhancing quality and minimising cost in addition to widening an effective financial landscape (The FinTech Revolution, 2015). Though numerous studies have been conducted, the motivations behind the study are identified from theoretical and empirical study points of view. Firstly, the phenomenal growth of FinTech in the sharing economy has a significant impact on the global financial industry, which is a competitive disadvantage for more than 83% of firms caused by the emergence of FinTech startups, especially in China and the U.S. (KPMG, 2015; PwC, 2016). In addition, according to Holland FinTech (2015) a revenue transaction (approximately \$660 billion) occurs from the traditional financial institute to these startups, and hence, to ensure competitive advantages, firms are required to invest in FinTech. The operations of fintech are increasing every year that it plays a prominent role in strengthening the economy by stimulating the digital economy with the help of technological innovation. By this way, centralisation of the financial activities of local government will accumulate. Here, by accumulating fintech and digital economy, local government can motivate the implementation of mutual development level (Chen, Teng, & Chen, 2022). Further, it will develop the quality of credit issue. Even from the perspective of environmental degradation, fintech assists in diminishing the carbon-dioxide effect, which will lead to the achievement of a ‘low-carbon economy’ (Tao, Su, Naqvi, & Rizvi, 2022). Secondly, the innovation of FinTech not only enhances the quality of financial services to its customers with its diversified financial services like mobile payment, peer-to-peer services, Robo-advisors, etc., but also ensures a financial upper hand by ensuring financial or economic benefit in risk-benefit analysis (Nguyen, 2022). During the financial crisis in commercial banks in terms of meeting the loan demand, the involvement of FinTech in SMEs operates as a remedy of the situation (Adeosun, Anagreh, Tabash, & Adedokun, 2023). Also, Mascarenhas, Perpétuo, Barrote, and Perides (2021) reveal that the risk in the FinTech is not considered by the Brazilian FinTech users, but they consider the early adopter’s economic benefits. Here, the benefits and risks are diversified. For example, for the early adopter, operational risk influences their financial performance, while in the case of the late adopter, it is a financial risk due to seamless investment. Furthermore, it has been disclosed that through the digitalisation of the public finance activities, the government can improve the operations of public finance with improved information technology, which will enhance the speed of government transactions (Uña, Verma, Bazarbash, & Griffin, 2023). Better fiscal transparency and budgetary planning can be ensured with the help of high-frequency information technology processes, including resource allocation. A multi-diverse FinTech service

ensures financial stability in BRICS (Brazil, Russia, India, China, South Africa, Egypt, Ethiopia, Indonesia, Iran, and the United Arab Emirates) countries (Vuković, Hassan, Kwakye, Febtinugraini, & Shakib, 2024). However, these revolutionising blockchain technologies have faced some challenges in FinTech investment management, customer management, technology integration, and so on (Lee & Shin, 2018). Among all of these challenges, security challenges in mobile phones are detrimental to the FinTech industry. Significant data storage in mobile phones, including information related to payment applications, can be jeopardized. In Hayashi (2016) the Consumer Financial Protection Bureau (CFPB) compelled Dwolla to pay a penalty for its data security breaches and misleading cybersecurity. Thirdly, despite several benefits, FinTech has provided an opportunity to increase the rate of financial crimes. The study will assist potential business leaders in understanding the classification and method of these crimes. By leveraging financial technologies, criminals are using FinTech in money transfer, fraud, money laundering, etc. (Nikkel, 2020). By studying the nature and method of financial crime, it will be easier to reduce the rate of financial crime by improving the financial information technology. For example, the lack of regulations and maximisation in the usage of cryptocurrencies encourages the perpetrators to abuse the FinTech (Despotović, Parmaković, & Miljković, 2023). To ensure the limits of legality among the economic users, an organic regulation like an anti-money laundering legal framework is developed (Faccia, Moşteanu, Cavaliere, & Mataruna-Dos-Santos, 2020). Yet, the regulatory loopholes in this advancing information technology in the financial area often generate obstacles to financial inclusion. The fraud triangle approach (motives, opportunities, and rationales) confirms the involvement of financial crimes in such regulatory loopholes (Zakaria, 2023). According to Saluja (2024) during the COVID-19 period, financial crimes, especially “identity theft,” have increased at an enormous rate. At last, due to a lack of skilled developers, with the growth of FinTech, the rate of customer vulnerability is also enhancing at a rapid rate (Sampat, Mogaji, & Nguyen, 2024). Ineffective data management increases customer vulnerability due to the lack of developed applications for mobile phone users and lack of proficiency among developers. Moreover, improper integration between the new technology and the traditional one is another reason for which customer management becomes weak and the organisation loses competitive advantages (Lee & Shin, 2018). By the study, it will be easier for responsible authorities to identify the financial obstacles or financial crime or regulatory loopholes and then, to innovate effective information technology and formulate regulations to reduce financial loss.

FinTech has a prominent impact on the economy of the world. It has become a major player in the financial world. It has increased as a great phenomenon that in 2016 a 63% increase in the investment in the FinTech industry has been shown (Accenture, 2016). Several researchers have studied numerous dimensions of FinTech. However, as the operations of FinTech are widening day by day, both as a blessing and a curse, they are not comparable in the existing literature. With the improvement of Fintech, not only will the possibility of financial crime increase, but there will also be enhanced information technology to identify and mitigate those crimes. Yet, there are few studies that have been conducted on this matter. As fintech is playing a prominent role in both mitigating and increasing financial crime, there is not enough study that provides any established or final verdict. Hence, the aim of our study is to investigate the dual impact of FinTech by analysing the financial crimes, their mechanism, and their impact with a case study. Also, it will come to the decision that whether fintech is a curse or a blessing in terms of financial crime.

The study explores the dual role of fintech in enabling and combating financial crime. Therefore, the influence of fintech on the acceleration and vulnerability of financial crime has been investigated that highlights the impact of financial information technology on the landscape of financial crime in financial institutes, including economic, operational, and reputational aspects. By scrutinising several case studies, the role of fintech both in exacerbating and mitigating financial crime has been revealed. Several technological innovations that are developed to ease financial activities have been elucidated. Moreover, it is given to the fact that financial crime has become more pervasive with the proliferation of financial technology; the study discloses current, emerging, and international

regulatory trends to mitigate financial crime along with the method of financial crime. Analysing the method of financial crime will assist potential academicians and businessmen to understand the context of financial crime and how to counterfeit it with the help of novel innovations and regulation. Furthermore, the study provides a benefit and risk analysis to provide an acknowledgement of multifaceted technological advantages and a balanced and nuanced view of the financial role.

To obtain the objection, in our study, we demonstrate a trend analysis and an in-depth analysis of key technologies in Chapter 2. In the third chapter, we apply the fraud triangle approach in fraud analysis and hence, the investigation of financial crimes, its mechanism, and the social impact is shown. Along with the challenges of FinTech, the fourth chapter elucidates the steps of FinTech's crime prevention strategy in a theoretical way. However, the negative impact is also analysed in the next chapter. Chapter 7 manifests some cases of the implementation of the technology both as a blessing and a curse. Next, a trend analysis of the regulatory framework for governing FinTech, financial crimes, and risks is given. Chapter 8 is about the balancing act between financial benefits and risks that are identified. An analysis of the future outlook is illustrated in a theoretical way in chapter 9. Chapters 10 and 11 are about conclusion and implications, respectively.

## 2. THE LANDSCAPE OF FINANCIAL TECHNOLOGY (FINTECH) HISTORICAL CONTEXT

### 2.1. Definition and Evolution of Financial Technology

The adaptation of digitalisation in the financial sector leads to the path of information technology development, which is known as "FinTech", an IT-induced financial product (Lechman & Marszk, 2021; Puschmann, 2017). Numerous IT-induced transformation drivers have a significant influence. New models like crowdfunding and peer-to-peer investment accelerate the efficiency of information technology to ensure the quality of financial services through automation (Gomber, Kauffman, Parker, & Weber, 2018). In addition, the growth of the customer base has played a prominent role in resizing the channel management road to customers by implementing hybrid client interaction (Nüesch, Alt, & Puschmann, 2015). For the strategic importance of FinTech, the cost of IT is the second largest cost factor after labour cost, which is approximately 15% to 20% (Gopalan, Jain, Kalani, & Tan, 2012). Hence, the usage of IT in financial intermediaries, banks, and insurance companies has a long history.

Financial technology, known as FinTech, first emerged at the beginning of the 1990s (Hochstein, 2015). According to Arner, Barberis, and Buckley (2015) and Puschmann and Alt (2016) the phases of information technology development in the financial sector are sectioned into three areas, which are internal digitalisation, provider-orientated digitisation, and customer-orientated digitisation.

**Table 1.** Evolution of fintech technology.

Area	Internal digitalization			Provider-oriented digitalization	Customer-oriented digitalization
Focus	Phase 1 (Until 1960)	Phase 2 (1960–1980)	Phase 3 (1980–2010)	Phase 4 (2010–2020)	Phase 5 (from 2020)
Strategy	Customer channel characterized as single	Two customer channels	Multiple customer channel	Cross customer channel	Hybrid customer channel
Organization	The process of system	Back-office process	Front-office process	Provider process	Customer process
System	No system is integrated	Partially integrated system	Internally integrated system	System integrated with external financial service provider	System integrated with external non-financial service provider

Source: Puschmann and Alt (2016) and Puschmann (2017).

Table 1 represents the evaluation of the FinTech covering 5 phases, starting from phase 1 in 1960 to phase 5 in 2020. For each phase, it included strategy, organisation, and system. For example, in phase 1, users connections

were mainly restricted to a single channel, and the strategy was just data entry and record keeping. And there was no opportunity for system integration. Phase 2 (1960-1980) was limited to two customer channels, and from then on, tech-based service increased, though the system was shared with a few people. Within the phase 3, the number of channels has been increased, and customers got service through online banking. In phase 4, service providers offered their service to the customers effortlessly by using cross-customer channels. And currently going phase 5, which is more convenient by using hybrid customer channels.

### *2.1.1. Internal Digitalization*

The first three phases are considered internal digitalisation, where internal processes like payment method and transaction recording are concerned. At first, in banks and financial institutes, a single channel characteristic is implemented, which develops into two customer channels and a front-office process. In the third phase, a multiple-channel approach is implemented (Gomber, Koch, & Siering, 2017; Matt, Hess, & Benlian, 2015; Puschmann, 2017).

Provider-Orientated Digitalisation: In this phase, to ensure a minimum degree of in-house production, integration of the process is focused. Reduction of in-house production enhances efficiency and streamlines operations (Bharadwaj, El Sawy, Pavlou, & Venkatraman, 2013). The services started from support areas like IT services (foundations of back-office operations), which reached back-office areas like payment methods, transactions, and bank accounts (Gozman, Liebenau, & Mangan, 2018). A standardised process and application functions are prime concerns in reshaping the functions of financial institutes and implementing digital transformation strategy (Matt et al., 2015).

### *2.1.2. Customer-Oriented Digitalization*

The functions of this phase are centred around customers. The hybrid customer channel (a broader perspective of the channel) and customer process are the centre for the design of financial products and services, like a peer-to-peer model, and the development of non-financial service providers to enhance customer satisfaction and experience (Verhoef, Kannan, & Inman, 2015). Therefore, optimisation of customer process will enhance the financial product and service delivery (Matt et al., 2015).

## *2.2. Key Technologies of FinTech*

### *2.2.1. Blockchain and Distributed Ledger Technology*

The empowerment of public and private sector computing applications has been ensured through the implementation of blockchain technology. Here, with the validation of multiple nodes, the technology complies with the cryptographic audit trail in a distributed audit trail. In addition, determining assets and agreements through the application of a common protocol reduces many third-party verification processes (Treleaven, Brown, & Yang, 2017). A distributed ledger is recognised as a decentralised system, secured through a cryptographic method that shares, replicates, and synchronises the transaction records to parties (Antal, Cioara, Anghel, Antal, & Salomie, 2021).

### *2.2.2. Artificial Intelligence and Machine Learning*

Investment decisions, taken by discretionary portfolio managers, have been taken on the basis of raw information or intuition for which the degree of failure in quantitative finance is higher. Therefore, machine learning in constructing financial decisions plays a prominent role. There are data curators who are responsible for collecting, indexing, and storing data, and also, the data is aligned in a tabulated or hierarchical manner. Furthermore, this FinTech technology is implemented in algorithm trading, fraud detection, risk management, and so on (De Prado, 2018; Kulkarni, 2023).



### 2.2.3. Robo-Advisor and Automated Financial Planning

In Sironi (2016) the collaboration between finance and technology is elucidated with the term “financial technology companies.”. Here, in this section, Robo-advisor has a significant influence in reshaping goal-based behaviour by turning it into goal-based, cost-effective decision-making (Koistinen, 2023). This automated investment solution-making tool applies an investment philosophy of individual-centred. A strong interaction between individuals, advisors, and final investors is established to determine the risk tolerances with the help of this game-changing automated tool.

Big Data and Data Analytics: Chen, Mao, and Liu (2014) argued that big data is classified as “massive data,” which is improperly captured, recorded, obtained, and merged. Apache Hadoop identifies big data as datasets that are not maintained or captured within a satisfactory scope by general computers. Data analytics tools assist project managers to develop data-driven decisions, predict trends, and so on, which enable project managers to implement project analytics (Uddin, Ong, & Lu, 2022).

### 2.2.4. Mobile Payment and Digital Wallet

In 1997, with the first transaction by mobile payment, researchers started the research about the financial and operational impact of these transactions (Dahlberg, Guo, & Ondrus, 2015). Another study claims mobile payment is the source of payment for goods and services through wireless connections (Chen, 2008).

Biometric and Security Technologies: For enhancing perceived security, FinTech companies should develop biometric identification technology. Fraud detection has become a crucial point for every company to enhance and establish the quality of services and effectiveness. The biometric recognition technologies and their implementation affect the FinTech security through fingerprint, voice, and facial recognition (Wang, 2021).

### 2.2.5. Regulatory Technology

RegTech is a significant portion of FinTech that refers to the incorporation of information technology in monitoring, reporting, and compliance in regulation (Arner, Barberis, & Buckey, 2016). Establishing a safer and more efficient financial system is considered the prime concern for financial companies and regulators to analyse the financial section. Therefore, a strong and efficient risk management and cost-effective tool can be used as an economic incentive in FinTech companies.

### 2.2.6. Cloud Computing

The convergence of IT efficiency and business agility is recognised in cloud computing, where IT efficiency refers to the efficiency of modern computers with highly operational hardware and software, and business agility refers to the usage of IT as a competitive tool (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011). With the implementation of cloud computing, reduction in information asymmetry and limitations of finance have been ensured in FinTech companies, and moreover, it enhances the activities in the utilisation of resources, green economic activity, and sustainable economic development. Furthermore, the implementation of cloud computing provides assistance in scalability, cost-efficiency, and the rapid development of new applications and services (Lăzăroiu et al., 2023; Macchiavello & Siri, 2022).

## 2.3. Trends in FinTech Adoption and Innovation in Financial Institutions

FinTech is an umbrella term for the technology-based innovative services to develop financial services and business models to improve the process, delivery, and services with a prominent impact on financial markets and implementation. It has turned into a global phenomenon for the researcher, business leaders, and academicians (Chinnasamy, Madbouly, & Reyad, 2021; Mention, 2019). In the broad array of technology-based financial services, some key trends in the adoption and innovation of FinTech within financial institutions are mentioned:

### 2.3.1. Digital Transformation and Innovation

A new competition by FinTech companies causes existing challenges faced by the traditional banking environment. The convergence between emerging business models and technology improves streamlined operations and customer satisfaction (Gomber et al., 2017). A digital finance cube is innovated with the consensus of business operations, technologies, and technological concepts, which has significant influence over various stakeholders from three dimensions (consumers, market players, and regulatory font) (Sangwan, Prakash, & Singh, 2020).

### 2.3.2. Blockchain and Cryptocurrencies

Blockchain is a peer-to-peer network or a decentralised network environment with a shared ledger that is connected by nodes (Sarmah, 2018; Tapscott & Tapscott, 2016). The consensus between blockchain and FinTech is a lack of service quality in the development of necessary software development products for startups. Blockchain provides credit or liquidity risk management services through an autonomous system. Moreover, it revolutionises the traditional banking system through security, efficiency, and transparency (Fernandez-Vazquez, Rosillo, De La Fuente, & Priore, 2019).

### 2.3.3. Artificial Intelligence and Machine Learning

Investment decisions that are taken by discretionary portfolio managers often count on raw information or intuition, resulting in a higher risk of failure in quantitative finance, especially in the case of establishing investment policy. Consequently, machine learning plays a crucial role in shaping financial decisions. Data curators are responsible for gathering, indexing, storing, and organising data in tabulated or hierarchical formats. This FinTech technology is also applied in algorithmic trading, fraud detection, risk management, and other areas (De Prado, 2018; Kulkarni, 2023).

### 2.3.4. Open-Banking and API Integration

Switching to a financial product or service requires a cost (known as “switching cost”), which is the prime switching inertia of consumers and new providers of banking services in the United Kingdom (Borgogno & Colangelo, 2020). From this point of view, the term “open banking” has arisen, which depicts a financial technology to implement regulation so that banking consumers reduce the switching cost and maintain their accounts (Chan, Troshani, Rao Hill, & Hoffmann, 2022). However, open banking allows its providers to share greater information with other providers, while traditional banking is based on the principle of a “closed and fragmented system.”. Therefore, it increases the degree of fraud and customer privacy breaches (Mah, 2020).

### 2.3.5. Mobile Banking and Payment Solution

Mobile banking has a vital role in elevating poverty by the inclusion of all social groups into economic growth. It has become a crucial tool for transforming society into a cashless one that enhances customer engagement and service delivery (Dahlberg et al., 2015; Yahaya & Ahmad, 2018). In the FinTech business, mobile banking has significant influence through large investments. Here, by analysing the big data, this technology focuses on consumers and has the advantage of international technical support and bilateral cooperation (Le, Mai, Phan, Nguyen, & Le, 2021).

### 2.3.6. Peer-to-Peer Lending and Crowdfunding

FinTech, a technology-based business model innovation, revolutionises the traditional process of financial product and service delivery (Philippon, 2016). There are two alternatives to financing channels, which are peer-to-peer lending and crowdfunding. Here, peer-to-peer lending (another term is “social lending”) refers to the process of

collaborating borrowers and lenders online at lowering interest rates. While, in the “crowdfunding” approach, a small amount of capital is raised from the small project and lent to the pool of users in a loan-based manner through an online platform (Ghazali & Yasuoka, 2018; Gupta, Raj, Gupta, & Sharma, 2023).

### 2.3.7. Cloud Computing

The union of information technology (IT) efficiency and business agility is epitomised in cloud computing, where IT efficiency pertains to the performance of modern computers with advanced hardware and software, and business agility involves using IT as a competitive advantage (Marston et al., 2011). The adoption of cloud computing in FinTech companies has shrunk information asymmetry and financial constraints while also augmenting resource utilisation, promoting green economic activity, and supporting sustainable economic development. Additionally, cloud computing offers benefits such as scalability, cost-efficiency, and the rapid development of new applications and services (Lăzăroiu et al., 2023; Macchiavello & Siri, 2022).

### 2.3.8. Internet of Things (IoT) in Financial Services

IoT consists of two words, and these are “Internet” and “Things.”. The Internet of Things depicts a connection of objects with identifiable addresses that operate as traditional information carriers (Abdul-Qawy, Pramod, Magesh, & Srinivasulu, 2015; Gubbi, Buyya, Marusic, & Palaniswami, 2013). The connection among existing objects, intelligence sensors, smart objects, traditional computing networks, and others enables the recording, generating, and exchange of data within data centres or network clouds, which assist project managers to operate complex and computational tasks in independent decision-making without human intervention (Botta, De Donato, Persico, & Pescapé, 2016).

## 3. FINANCIAL CRIMES

### 3.1. Overview of Financial Crimes

The Organisation for Economic Co-operation and Development (OECD) is a key international standard-setting organisation that conducts valuable independent analysis and statistics on a range of economic and other policy areas. The rise of financial crime in the OECD has caught the attention where the term “economic crime” is more commonly used. Here, ‘financial crime or economic crime’ indicates a range of criminal activities, including money laundering, mass-marketing fraud, or tax evasion, which result in the financial losses (Achim & Borlea, 2020; Nicholls et al., 2021; Ünvan, 2020). At first, fraud was considered a financial crime (prior to the 21<sup>st</sup> century), but from the late 1980s, money laundering or insider dealing also fell into the category. Furthermore, crimes involving intellectual property will be included as financial crimes if they have a significant influence in “predicting crime” (Levi, 2015).

For a better understanding of the causes behind financial crime, the study requires a theory development. When a set of interrelated constructs, definitions, and propositions form a methodical view of phenomena and postulate the relationship between variables through case study, it is referred to as “theory development (Amadi, 2023; Gottschalk, 2010). The theoretical streams of financial crime have been divided into behavioural theories, organisational theories, and managerial theories (Amadi, 2023). Examining the perception of the individual behind the financial crime is the prime concern of behavioural theory. Hansen (2009) depicts that such kinds of elite crimes are organised by the individual within the organisation for their own personal enrichment. Another theory, organisational theory, elucidates that committing a crime requires a monopoly and official intervention where the framework and organisation of crime occur (Chang, Lu, & Chen, 2005; Christie, 1969). Finally, managerial theory refers to the inclusion of management in financial crime.



### 3.2. Classification of Financial Crime

Financial crime encompasses a wide range of illegal activities with the usage of money and financial instruments. Thus, it is critical to classify these crimes to set effective regulations, prevention policies, and enforcement of rules. The classification of financial crime is explained:

#### 3.2.1. Fraud

Fraud and violation of trust often distort the central role of trust in market facilitation (Palmer, 2008; Yenkey, 2018). Traditionally, fraud encompasses deceit or misrepresentation of deceptive financial disclosure through unauthorised usage of credit cards (credit card fraud), deceitful claims against insurance (insurance fraud), unauthorised transactions within financial institutes (bank fraud), and so on (Reurink, 2018).

#### 3.2.2. Money Laundering

Apart from the official economy, the criminal economy is a part of the underground economy that seeks to annihilate the business environment through illegal transactions for financial advantages (Schneider & Windischbauer, 2008). Hence, money laundering (originating from the US) is the process of laundering money or profit acquired from criminal activities like acquisition and possession of criminal activities (Korejo, Rajamanickam, & Said, 2021).

#### 3.2.3. Insider Trading

An inefficient market for public company stock that trades established on material and non-public information for unlawful reasons is diagnosed as “insider trading” (Bhattacharya & Daouk, 2002). The unequal distribution of information often provides individuals with a higher financial advantage than general people.

#### 3.2.4. Bribery and Corruption

One of the most significant impairments in the development of a country is bribery, the worst form of corruption. There is a lack of comparability between the revenue stemming from bribery and the cost of it (Loughman & Sibery, 2011). The main motivation behind such financial crime is known as efficient corruption, bribery to reduce the bureaucratic system (Fisman & Svensson, 2007).

#### 3.2.5. Tax Evasion

Tax evasion is an illegal framework of tax when an individual does not present the information relating to revenue stemming from labour and capital (principle taxable) (Sandmo, 2005). Such kind of financial crime is known as a federal crime, and a person committing tax evasion is subjected to a prison sentence (Slemrod, 2007).

#### 3.2.6. Cybercrime

Cyberspace has been used as a financial crime with the usage of financial and hacking tools for annihilating social engineering for illegal economic gain. Here, the term “cybercrime” is introduced, which encapsulates all of these factors (Hasham et al., 2019). The profit-driven cybercrime compels financial institutes like banks to use in-house-developed tools for the protection of financial information (Nicholls et al., 2021).

### 3.3. Methods and Mechanism of Financial Crime

Determining the methods of financial crime is the pillar of developing mitigation strategies. On the other hand, different financial crimes have different mechanisms by which benefactors ensure illicit cash flow.

### 3.3.1. Fraud

Embezzlement, Ponzi schemes, and accounting fraud are the most common methods of fraud to acquire illegitimate gain. Embezzlement is the process of misappropriating funds or assets through falsifying records, diverting funds, and generating fake expenses by the employees. The unauthorised use of funds and assets leads to breaches of trust where the fund from normal operations is used as an illegitimate financial gain for embezzlers (Medhi, Singh, Goswami, & Singh, 2024). Another method of financial fraud is a Ponzi scheme, where the profit of shareholders is provided from the capital of new shareholders rather than the profit from operations. Accounting fraud is the process of manipulation of financial information (inflating reimbursement, concealing expenses, and misstating assets and liabilities) to represent a false picture of financial health (Bhasin, 2016; Chorvatovičová & Saxunová, 2016).

### 3.3.2. Money Laundering

The rate of money laundering is enhancing along with the advancement of information technology. It is the process of transferring illicit cash flow for financial gain (Korejo et al., 2021). At first, in the placement phase, by cash deposits, wire transfers, and purchasing high-value assets, perpetrators introduce illicit funds into the financial system (Villányi, 2021). Then, in the layering phase, to obscure the origin of the fund, a complex scheme of wire or financial transactions, like foreign money orders, offshore accounts, and multiple transactions, are made. Finally, in the integrating phase, by investing in real estate and luxury goods, the laundered money is integrated into the economy, which is difficult to distinguish (Boles, 2017).

### 3.3.3. Cybercrime

Phishing, ransomware, and hacking are the methods of cybercrime. Phishing is the process of obtaining sensitive information by entering as a trustworthy entity in the electronic community (Alkhalil, Hewage, Nawaf, & Khan, 2021). On the other hand, ransomware, malicious software, encrypts the data of the victim and demands ransom to restore access (O'Kane, Sezer, & Carlin, 2018). Unauthorised access to computer systems to steal, alter, or destroy data or to disrupt operations is known as "hacking" (Goni & Alam, 2022).

### 3.4. Impact on Financial Institutes

There is a multifaceted and profound impact on financial institutions due to the increasing rate of financial crime. As financial crime encapsulates a wide range of illegal activities, it has a significant influence (both directly and indirectly) on financial institutes. Here, some of them are depicted.

Figure 1 demonstrates the impact of financial crimes on financial institutions. Direct financial losses, operational impact, strategic and competitive impact, and reputational damage are the major financial crimes.



Figure 1. Impact of financial crimes on financial institutes.

#### 3.4.1. Direct Financial Loss

Financial institutes face monetary losses for the occurrence of financial fraud and embezzlement. Financial misconduct leads to the financial failure of the misconduct of financial controller (Tomasic, 2011). Therefore, the amount of investment in the productive sector often lessens which erodes the profitability of financial institutes and thus, the path ends with the erosion of net worth (Gelb, 1989).

#### 3.4.2. Reputational Damage

When an organisation is subjected to sanctions for misleading financial information, shareholders are the most vulnerable stakeholders that face financial loss, including a decreasing share price. Furthermore, according to the Basel Committee of Banking Supervision, the financial institute has to face stricter regulations and higher compliance costs (Karpoff, Lee, & Martin, 2008; Supervision, 2011).

#### 3.4.3. Operational Impact

Senior corporate managers of the financial institutes have to breach compliance with the regulations. Hence, there is a requirement for both technological and intellectual resources for efficient operation (Tomasic, 2011). In addition, certain services and operations may not be available due to the investigation of financial crime like white collar crime (Pickett & Pickett, 2002).

#### 3.4.4. Strategic and Competitive Impact

After the investigation of financial crime, the financial institutes will face the reduction of competitive edge due to financial disruption or economic damage and losses of market share (Crockett, 1996; Financial Crisis Inquiry Commission, 2011). To revive from the situation, a long-term strategic solution, consisting of a new business model and technology, is required.

### 3.5. Social and Economic Impacts for Individual, Corporation and Whole Economy

The social and economic impact of financial crime is extensive, and it widens the social and economic challenges along with the reduction of the confidence of investors. Individuals may suffer direct financial losses like asset erosion and credit card fraud due to identity theft and cybercrime (Nicholls et al., 2021; Reurink, 2018). Along with psychological impact (anxiety and stress due to lack of security), it will have a detrimental impact on victims. On corporations, the multilevel impact of financial crime is divided into direct financial loss, reputational losses, operational impact, and strategic and competitive impact. Organisations suffer monetary losses due to incidents of financial fraud and embezzlement. Such financial misconduct can result in the financial downfall of those responsible for overseeing financial activities (Gelb, 1989; Tomasic, 2011). Furthermore, they lost the trust of the shareholders and investors, which caused reputational or social damage. Financial crime has an extensive negative impact on the economy. Financial or economic crimes are the portion of both individual and structural variables (Saddiq & Abu Bakar, 2019). Crimes like corruption disrupt the social welfare of developing and emerging countries, which lowers economic growth (Uma & Eboh, 2013). In financial crime, benefactors are the organisations or noteworthy figures, and victims are individuals or clusters of individuals who bear the economic cost (Saddiq & Abu Bakar, 2019). Therefore, the economic inequality between benefactors and victims is widened. In addition, money laundering and corruption can undermine economic development and stability (Bartlett, 2002).

## 4. POSITIVE IMPACTS OF FINTECH ON FINANCIAL CRIME PREVENTION

### 4.1. Enhanced Fraud Detection

AI plays a major role in cloud-based FinTech apps' ability to avoid fraud. Large-scale datasets may be processed by machine learning algorithms, which can identify patterns linked to criminal actions, including credit card fraud,

identity theft, and account takeovers. AI systems get better at identifying new fraud strategies by constantly learning from fresh data (Kunduru, 2023). The likelihood of financial fraud has increased due to the expanding use of digital payments. As a result, National Payment Switches (NPSs), which are directly owned by Central Banks (CBs), are incorporating cutting-edge technology like cognitive computing more frequently to improve their capacity to identify fraudulent activity within their nations (Roszkowska, 2021). AI technologies, such as machine learning (ML) and deep learning (DL), have completely changed how fraud is detected and stopped. FinTech businesses can now handle enormous datasets, identify intricate fraud patterns, and anticipate fraudulent transactions with previously unheard-of accuracy and efficiency by utilising AI. This enhances the safety of financial transactions and guarantees a reliable and easy-to-use experience for users (Philip Olaseni Shoetan & Babajide Tolulope Familoni, 2024). Real-world instances, like the Federal Bureau of Investigation (FBI)'s Financial Crimes Section's identification and stop of massive fraud schemes, demonstrate the vital role that machine learning and big data play in safeguarding the country's financial borders (Saxena & Vafin, 2019).

#### 4.2. Improved Transparency

FinTech sets a realistic objective of considerably increased and sustained financial inclusion by drastically lowering the cost of delivering financial services. Simultaneously, increased automation, streamlined operational procedures, and more sophisticated and affordable analytics provide the possibility of promoting improved openness while preserving or enhancing individual privacy and financial activity security. Improved consumer protection, financial regulation, and oversight would all benefit from such transparency (Barr, Gifford, & Klein, 2018). A degree of traceability and transparency made possible by blockchain technology is naturally advantageous to improved governance. Because every transaction on a blockchain is captured on an immutable distributed ledger that is available to all network users, it is easier to audit and follow transactions to ensure they comply with legal requirements (Okunleye, 2024).

#### 4.3. Automated Compliance

FinTech organisations have benefitted from robotic process automation (RPA), which has enabled workers to concentrate on higher-value jobs by automating monotonous labor. Efficiency has grown as a result, and customer satisfaction has gone up. FinTech businesses have been able to create better financial goods and services by using big data analytics to acquire insights into client behaviour and preferences. Biometrics has been significant in lowering the risk of fraud and enhancing the security of online financial transactions (Jain, Prajapati, & Dangi, 2023). Many tools for automating compliance and monitoring activities have been created or suggested to improve their efficiency. The reviewed studies offered automated reporting tools, digital wallet supervision and auditing tools, more effective Know Your Customer (KYC) processes, and automated fraud detection (Koskipää, 2022). North Carolina Department of Public Safety (NCDPs) are frequently used by businesses to expedite the creation of cloud-based apps while maintaining alignment with corporate strategy. On low-code or no-code systems, for instance, audit trails and document creation may be automated, ensuring and enhancing compliance. FinTech businesses and financial institutions that need to react fast to changes in the market will find this to be very helpful (Fong, Han, Liu, Qu, & Shek, 2021).

#### 4.4. Blockchain Integrity

Blockchain technology is gaining popularity across a range of sectors due to its promise to revolutionise data security and transaction integrity. It is most recognised for being the foundation of cryptocurrencies like Bitcoin. FinTech businesses may use blockchain to develop trustless systems—systems where trust is ingrained in the technology itself. The transparent nature of blockchain also helps with regulatory compliance since it creates an unchangeable, transparent record of every transaction (Mustyala, 2023). The integrity and resistance to tampering

of financial transactions are preserved by the immutable record of blockchain technology. Without network consensus, transactions on the blockchain cannot be altered or deleted. By reducing fraud, disputes, and mistakes, this feature enhances the auditability, accountability, and transparency of financial transactions (Yerram et al., 2021). The integrity, validity, and anonymity of the blockchain are safeguarded by the encryption algorithms and methods employed in blockchain technology, such as electronic signatures and Merkle trees (Nelaturu, Du, & Le, 2022).

#### *4.5. Increased Accountability*

Important questions are also brought up by the use of AI in fraud detection, such as moral dilemmas over data privacy and the possibility of bias in AI systems. These difficulties demand a well-rounded strategy that makes use of AI's advantages while guaranteeing accountability, transparency, and justice in its use (Philip Olaseni Shoetan & Babajide Tolulope Familoni, 2024). A developing policy issue in the current Open Government Partnership (OGP) action plans is digital governance. A greater number of members use government machine learning and artificial intelligence (AI) tools to concentrate on accountability. Open data has emerged as one of the most potent tools in the fight against corruption in recent years; therefore, using it and holding public procurement authorities accountable are the priorities (Lieonov, Bozhenko, & Mynenko, 2023). Through the use of algorithmic protections, disruptive general-purpose technologies can ensure that socio-economic requirements are satisfied more swiftly and reliably, based on a far larger range of patterns. Conventional regulation depends on big, centralised control organisations that utilise human (subjective) capabilities since it is founded on (sometimes vague and unworkable) regulations and their continuous accountability (Achim et al., 2023).

#### *4.6. Real-Time Transaction Monitoring*

Regulatory technology (Regtech) systems track online transactions in real time to spot anomalies or problems in the realm of digital payments. Any anomaly is reported to the financial institution so that it may investigate and ascertain whether fraud is occurring. Regtech can reduce the risks and expenses related to lost money and data breaches while also aiding in the identification of possible threats to financial security and stability (Zeidy, 2022). Monitoring or forecasting financial risks using intelligent agents is one way that FinTech is being used to enhance corporate operations. Before being transferred across the network, sensitive data is split into two portions so that privacy may be maintained even while enemies are keeping an eye on the transmissions (Gai, Qiu, & Sun, 2018). FinTech technologies can lower the cost of transactions. More precisely, the goal of blockchain and "smart contracts" is to lower the costs associated with enforcement and monitoring. Financial organizations create "internal sandboxes" where "smart contracts" may be thoroughly examined and tracked before being implemented on blockchain systems. Intermediaries have the authority to enforce contracts on behalf of any party, should the need arise, and can more readily oversee their performance than any one person can once they are signed (Panisi, 2017).

#### *4.7. Efficient Risk Management*

Risk management procedures are receiving a lot of attention from regulations and associated supervisory requirements, which in turn highlights the need for thorough, open, and auditable data analysis throughout enterprises. Big data analytics, artificial intelligence, and blockchain ledgers are examples of technologies that might more effectively handle risk management needs and related expenses (Giudici, 2018). Regtech and supervisory technology (suptech) are two examples of this. Regtech focuses on leveraging technology to help organizations manage their adherence to regulations, risk management, and regulatory duties (such as enhanced corporate reporting), whereas suptech helps deploy new technology to enhance supervisory and monitoring (Mnohohitnei, Scorer, & Shingala, 2019). FinTech, particularly big data and technology supervision, will



transform commercial banks' risk-management models and strengthen their risk-management capacities, ultimately lowering overall risk. Bank risk-taking is significantly influenced by risk management. Commercial banks may improve the efficiency, precision, timeliness, and stability of risk management—particularly in risk detection and assessment—by relying on financial technology (Li, Elahi, & Zhao, 2022).

#### 4.8. Enhanced Data Security

Data security, as defined by the International Standard for Information Security Management Systems (ISO 27002), is the availability, confidentiality, and integrity of data. The management and staff of FinTech companies are crucial in protecting data, which affects consumers' faith in these services (Stewart & Jürjens, 2018). The word "FinTech" has gained popularity to refer to cutting-edge technology that financial services firms have embraced. The approaches covered under this phrase range widely, from financial service delivery to data security (Gai et al., 2018). Financial data security and data protection are related to data interchange, and FinTech takes into account all other online hazards currently in existence (Mehrban et al., 2020). FinTech organizations can improve data security standards, foster consumer confidence, and mitigate the risks associated with cyberattacks and data breaches by implementing encryption solutions appropriately. Strict legal frameworks about data security and privacy must be followed by FinTech companies. Encryption methods that abide by legal criteria guarantee compliance and lessen the chance of fines or penalties (Omolara et al., 2024).

#### 4.9. Identity Verification

Biometrics plays a significant role in bolstering the identification of such security applications, particularly with the advent of FinTech, which exploits mobile devices and applications as promotional platforms. Nonetheless, people continue to worry about biometrics' privacy and reliability (Wang, 2021). Financial services firms employ several identification methods in FinTech apps to enhance fraud monitoring and user experience (Wang, Xue, Liu, & Pei, 2019; Zhu, Li, Wang, & Li, 2020). AI-driven biometrics can reliably confirm user identities by examining distinctive biological characteristics like fingerprints, facial features, and speech patterns. This makes it more difficult for unwanted parties to access private financial data. The potential of AI-driven biometrics in FinTech to strengthen security protocols is one of its main advantages. Passwords and PINs, which are considered traditional authentication techniques, are becoming more susceptible to fraud and hacking. Conversely, AI-driven biometrics uses an individual's unique biological features to provide a better level of protection. This greatly increases the difficulty with which scammers may obtain private financial data (Oseremi, Yinka, Nsiong, & Damilola, 2024). Some of the problems with passwords and/or personal identification numbers (PINs) can be solved by biometric technology. For instance, these technologies enable illiterate clients to use financial services such as payment processing (Hollanders, 2020).

#### 4.10. Anomaly Detection

Financial cybersecurity study and development may take a positive turn in the future with the combined use of anomaly detection and federated learning, which may greatly improve the safety record of FinTech systems. Every organization uses its data to train a local model, and it only updates the model when it receives updates from a central server, which combines all of the changes into a better global model. This decentralized methodology allows for a more thorough and generalizable approach to threat detection while mitigating the hazards associated with data centralization. Advanced anomaly detection techniques are essential for discovering fraudulent activity and system breaches when used in conjunction with federated learning (Noul & Hussain, 2024). ML includes anomaly detection methods that automatically recognize and categorize suspicious financial network data. To create models from a dataset, techniques including learning algorithms, statistical models, and artificial neural networks (ANN)

are employed. After that, the final representation is examined to determine the best practices and guidelines for preventing fraud (Stojanović et al., 2021).

## 5. NEGATIVE IMPACTS OF FINTECH ON FINANCIAL CRIMES

### 5.1. Increased Cybersecurity Threats

Phishing and malware assaults are two common cybersecurity concerns in the FinTech sector that put financial institutions and their clients at serious risk. Phishing attacks utilise a variety of strategies and tactics, such as phoney emails and websites used to obtain login credentials (Gupta, Arachchilage, & Psannis, 2018). These assaults have the potential to harm financial institutions as well as people by causing identity theft, financial losses, loss of personal data, and reputational harm to brands (Mohammad, Thabtah, & McCluskey, 2015). Financial institutions may suffer significant repercussions from these assaults, such as monetary losses, harm to their reputations, and regulatory scrutiny. Furthermore, cloud storage has been the focus of an increase in ransomware occurrences, which has prompted the development of machine learning-based hypervisor-level ransomware detection (Umoga, Sodiya, Amoo, & Atadoga, 2024). FinTech platforms hold sensitive financial information, including payment details, transaction records, and personal and financial data, which makes them appealing targets for fraudsters. The cybersecurity dangers that businesses in the sector confront are further increased by the interconnection of financial systems, the industry's reliance on outside providers, and the use of cutting-edge technology like cloud computing and mobile apps (Ungureanu & Filip, 2023).

### 5.2. Greater Anonymity in Transactions

Digital footprints are left by a variety of online activities. Since anonymity is only concerned with how to connect an individual to their purported identity, it is just a matter of institutional design and application administration. Similar to how deposited money is connected to bank accounts, enabling the real-name administration of anonymous banknotes, anonymity is not a necessary feature in digital finance, except for money laundering (Daofu, 2020). FinTech not only puts its users at risk, but also the interests of the general public. For instance, the anonymity offered by an international marketplace may encourage illegal misuse. Virtual currencies, like bitcoin, and the exchange systems that support them have developed into havens for blackmailers, tax evaders, drug and weapon traffickers, and money launderers (Lehmann, 2020).

### 5.3. Complexity in Tracking Digital Crimes

Data protection is the second main area of concern, which is highlighted by the growing importance of data in the financial industry. Distinct economies are developing distinct policies, some of which are reflective of essentially divergent social perspectives. The main instances of differing legal frameworks regarding the usage, ownership, and protection of data are the US, China, and the EU (Buckley, Arner, Zetsche, & Selga, 2019). To cover their traces and launder money that has been stolen, thieves use money mules. Sometimes, through online job portals or spam campaigns promising "earn extra money in your spare time!" People are recruited as mules in the hopes of obtaining part-time work as "financial intermediaries." After the money is deposited into the mule's account, it is assumed that they will take cash out, retain a certain amount, and send the remaining amount to another receiver (usually using a cash transfer service) (Nikkel, 2020). once identification information has been recorded, it is more difficult for hostile actors to tamper with or alter it due to the immutability of the blockchain ledger. Blockchain technology provides viable remedies for a range of issues of digital identification (Utkina, 2023).

### 5.4. Potential for Regulatory Gaps

The challenge that BigTechs provide to central banks' responsibilities and the data gaps that arise in connection with their operations are further implications. BigTech businesses are trying to establish themselves as

an important category of FinTech business. Along with significant benefits like economies of scale and the international reach of their platforms, these businesses also enjoy the advantage of user-generated data and advanced data analytics. The region's financial authorities have a dilemma in light of all of these possible data gaps resulting from growing FinTech activity in the banking system (Marqués et al., 2021). When consumer credit originates from the banking industry rather than FinTech, regulatory loopholes arise since supervisory frameworks tend to concentrate on this area. The financial ramifications encompass imprecise risk assessment as FinTech companies endeavour to precisely handle and apply the extensive array of data at their disposal, and plausible conduct issues culminating in extensive nonpayment when impoverished populations, especially the unbanked, obtain official credit for the first time. Numerous banks have expressed concern about the rise of FinTech firms. Additionally, they have publicly expressed their concerns regarding FinTech competition and regulations that adhere to the same strict guidelines. The sector is under attack because the lines have likewise blurred: FinTech is no longer the domain of established financial players, and regulators are no longer exclusively focused on financial institutions (Anagnostopoulos, 2018).

### *5.5. Rise of Sophisticated Fraud Schemes*

Deepfakes are an intriguing and captivating kind of faked and altered media. On the other hand, deepfakes cost FinTech firms a lot of money every year, and the problem is only getting worse. The consequences of identity theft and con artists affected 47% of all foreign enterprises in 2020. According to preliminary data for the fiscal year 2021, fraud rates are rising and con artists' methods are constantly becoming more complex (Saluja, 2024). Complex issues are also brought about by the digital revolution, especially in the area of financial fraud, which is becoming more common and sophisticated. The financial ecosystem is greatly impacted by the consequences of these fraudulent acts, which lead to significant financial losses and erode consumer trust (Saxena & Vafin, 2019). Consumers will now have to deal with the increased danger of fraud and scams in addition to cyber-insecurity. Vulnerable consumer groups suffer the most from scams. According to the National Council on Aging, older consumers are being targeted more often, and predatory behaviours that target those with impairments are also on the rise (Barefoot, 2020).

### *5.6. Vulnerabilities in Decentralized Systems*

Because blockchain uses cryptographic hash functions, transactions may be made tamper-proof, but attackers can still take advantage of other flaws. A malevolent opponent might be able to substitute or alter the input data without altering the digest if there is a collision in the hash algorithms. Unauthorized transactions might result from the forging of a signature (Nelaturu et al., 2022). To reduce users' need for reliable third parties, the majority of smart contract implementations are made with decentralized use cases in mind. Nevertheless, they frequently have the same flaws and vulnerabilities as the system's payments layer (Han, Huang, & Zhong, 2023). Because this platform offers an environment in which smart contracts may be executed, vulnerabilities that are exploited also give a malevolent opponent the ability to benefit without the connected parties' consent in the smart contract signature (Nelaturu et al., 2022). As with other FinTech technologies, smart contracts' hazards are not completely recognized because of their novelty. However, there are general factors to take into account when it comes to technological innovation and adaptation, such as where we are in the entire lifecycle. For example, if new technology is not extensively tested or used in real-world applications, defects and vulnerabilities may remain undiscovered (Duran & Griffin, 2021).

### *5.7. Challenges in International Cooperation*

One specific issue is the issuance and use of virtual currencies, which, if widely accepted, have the potential to alter the two main pillars that sustain the reserve currency status: the composition and dynamics of international

commerce and the impacts of the financial network. The requirement for reserves (buffered inventories and/or liquid assets) and the formation of new reserve currencies might be influenced by the liquidity and degree of confidence in the new cryptocurrencies. This will thus have an impact on foreign exchange and gold reserves, the exchange rate regime that is selected, and the dimensions and composition of the global financial safety net (GFSN) (St. Petersburg State University et al., 2020). Government-to-government implementing authorities (treasuries, banks, etc., depending on each state's administrative structure) pledge to hold regular (at least quarterly) working-level discussions (with political officials, legal experts, and regulators in attendance) to discuss the development of FinTech policies in each jurisdiction. This often entails promptly informing people about crucial FinTech-related news. These channels allow for the exploration of the perceived difficulties faced by FinTech companies in the nations set to sign FinTech bridge agreements (Tache, 2022).

### *5.8. Exposure to Digital Payment Frauds*

FinTech is becoming more externally visible, raising cyber vulnerability, in contrast to the rising reliance on intricate digitalized information technology hubs without replacement. These security holes can be used by cyber attackers to compromise data at custodian banks or Central Securities Depositories, interfere with payment systems, or destroy equipment that supports the financial system (Buckley et al., 2019). The likelihood of financial fraud has increased due to the expanding use of digital payments. Because of this, NPSs—which are directly owned by Central Banks (CBs)—are progressively using cutting-edge technology, such as cognitive computing, to improve their capacity to identify fraud in their nations (Alessio Faccia, 2023). The need for payment security is growing as a result of an increase in card fraud losses and data breaches, which cause financial institutions to suffer both direct and indirect costs. Users of payment handling software may become irritated by the more stringent security measures used in electronic payment systems (Ramesh, Amudha, Prasob, & Kanna, 2023).

### *5.9. Proliferation of Dark Web Activities*

Investigating cyber-related money laundering crimes is made more difficult by the widespread usage of encryption technology and the anonymity offered by the dark web. Although encryption is necessary to protect legal communications, it may also be a dangerous tool for cybercriminals trying to hide their illegal activity. A safe refuge for many types of illegal financial activity, the dark web offers untraceable transactions and encrypted communication methods (Bin Azero et al., 2024). Robust privacy and defence against government monitoring are offered by the Dark Web. People who live under repressive regimes that restrict free speech, prohibit access to huge portions of the internet, and prohibit criticizing government actions are drawn to the network. Because of the Dark Web's robust anonymity and plethora of identity masking strategies, thieves frequently use it to market and deliver their goods (Dhali, Hassan, Mehar, Shahzad, & Zaman, 2023).

## **6. CASE STUDIES**

### *6.1. Successful Implementation of FinTech in Crime Prevention*

#### *6.1.1. Enhanced Fraud Detection with AI-Powered Solutions*

One prominent example of successful FinTech implementation in fraud prevention is the ARIC™ Risk Hub developed by Feature space. This AI-powered platform employs adaptive behavioral analytics to build detailed profiles of genuine customers by analyzing transaction data and third-party information. This approach allows for near-real-time anomaly detection, identifying fraudulent activities within milliseconds. Deployed across 70 major financial institutions, ARIC™ Risk Hub has been reported to block 75% of fraud attacks, safeguarding over 500 million consumers globally. The adoption of such AI-driven systems has significantly reduced financial losses and operational costs, illustrating the transformative potential of FinTech in crime prevention (NVIDIA, 2022). The AI capabilities of ARIC Risk Hub enable it to analyze vast amounts of data quickly and efficiently, learning from each

transaction to improve its fraud detection accuracy continuously. This dynamic and adaptive approach not only protects consumers but also helps financial institutions stay ahead of increasingly sophisticated fraud schemes (NVIDIA, 2022).

### *6.1.2. Blockchain Technology for Enhanced Transparency*

Transparency and accountability in financial institutions have been significantly enhanced by blockchain technology. Blockchain creates an immutable ledger, ensuring that record-keeping transactions remain honest and transparent because all actions are permanently recorded on the chain. This technology has been effectively used in money laundering prevention and regulatory scrutiny. Specifically, financial institutions that utilize blockchain technology to monitor transactions have experienced greater efficacy in detecting and preventing fraudulent activities (McKinsey & Company, 2021a).

In cash transactions, blockchain technology increases validity as every small transaction made is recorded and cannot be altered in the future. Due to these features, this tool has significant value in safeguarding the integrity of financial documentation and compliance with various legal requirements. Because of its structure, blockchain provides greater transparency, allowing for the immediate detection of inefficiencies and potential crimes (McKinsey & Company, 2021b).

### *6.1.3. Real-Time Transaction Monitoring*

Another sector in which FinTech has proven effective is real-time transaction monitoring. PSPs have integrated sophisticated computational models to identify fraudulent transactions based on real-time assessments. It can detect abnormal procedures or transactions as the algorithm follows transactional patterns. To monitor and detect internal unethical behavior, PSPs have incorporated these advanced systems to manage better financial crime risks (McKinsey & Company, 2021a).

Real-time monitoring systems enhance the ability of PSPs to catch fraudulent activities as they occur. As transactions are processed, these systems scrutinize transaction details for signs of potential fraud, such as substantial withdrawals or transfers that deviate from a customer's regular activity. This proactive fraud-tracking and detection strategy enables financial institutions to mitigate losses and implement better safeguards more securely (McKinsey & Company, 2021a).

## *6.2. Instances of FinTech Exploitation by Criminals*

### *6.2.1. Rise of Sophisticated Fraud Schemes*

While fraud prevention technology has evolved, criminals have also leveraged advancements in FinTech to become even more sophisticated in their schemes. For instance, the evolving nature of crimes has given rise to vectors such as identity theft and fraudulent account creation, mainly due to the increased use of digital payment platforms. Digital onboarding is a significant weakness for digital scammers who fabricate fake identities and gain unauthorized access to financial services. This has led to substantial financial losses and has proven challenging for institutions to maintain robust security (NVIDIA, 2022).

### *6.2.2. Cryptocurrency and Money Laundering*

Another aspect regarding cryptocurrencies is the anonymity these currencies provide. Criminals have exploited the ability to anonymously transfer money online using cryptocurrencies, including laundering illicit gains and moving currency across borders in cybercrime activities. Since blockchain technology is decentralized, it poses challenges when regulatory authorities attempt to track and eliminate such activities. Although data on these categories is limited, numerous instances of money laundering through cryptocurrencies have been reported worldwide, highlighting our limited understanding of this risk (McKinsey & Company, 2021a).



### 6.2.3. Dark Web Activities

FinTech has also made financial crimes more pervasive through the proliferation of dark web activities. Cybercriminals use the dark web to trade stolen data, counterfeit money, and other illicit products and services. This underground economy thrives on the overarching pseudonymity and security offered by FinTech platforms, which significantly complicates law enforcement efforts to track and dismantle these criminal networks. Over the decades, the dark web has increasingly been associated with financial crimes, according to various reports, suggesting the need for much stricter monitoring and enforcement (Home of FinTech & Banking News, 2021).

## 7. REGULATORY LANDSCAPE OF FINTECH AND FINANCIAL CRIMES

### 7.1. Current Regulatory Framework

The regulatory landscape for FinTech and financial crimes is complex and multifaceted, with numerous laws and regulations designed to maintain economic stability, protect end-users, and prevent illicit activities.

In the U.S., various agencies have regulatory jurisdiction. These laws include regulations that can lead to technical non-compliance, such as the Anti-Money Laundering (AML) legislation, exemplified by the Bank Secrecy Act and the PATRIOT Act, which require financial institutions to create AML programs and report suspicious activities. The Securities and Exchange Commission (SEC) regulates issues surrounding securities, while the Commodity Futures Trading Commission (CFTC) oversees commodities. Additionally, the Office of the Comptroller of the Currency (OCC) supervises all nationally chartered banks (Tran & Kevin, 2023).

In the E.U. regulatory environment, the market structure is defined by directives like the Fifth Anti-Money Laundering Directive (5AMLD) and the Markets in Financial Instruments Directive II (MiFID II). These guidelines mandate thorough customer due diligence (CDD) and reporting of suspicious activities to prevent money laundering and terrorist financing. Furthermore, the General Data Protection Regulation (GDPR) tightly regulates data protection and privacy (Global Legal Insights, 2023).

The regulatory framework has evolved post-Brexit by introducing the Financial Services and Markets Act 2023, replacing retained E.U. laws with bespoke U.K. legislation. The Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) enforce compliance and ensure financial stability. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended in 2020) ensure that UK AML laws comply with international FATF standards (GOV.UK, 2023).

Table 2 represents the summary of nations, including the USA, European Union, and United Kingdom, that have enough regulations and regulatory forces to prevent financial crimes.

**Table 2.** Key regulations and regulatory bodies governing fintech and financial crimes.

Region	Key regulations	Regulatory bodies	Description
United States	Bank secrecy act (BSA)	Financial crimes enforcement network (FinCEN)	Requires financial institutions to implement AML programs and report suspicious activities.
United States	USA PATRIOT act	FinCEN, SEC, CFTC, OCC	Expands AML requirements, including mandatory information sharing and enhanced due diligence.
United States	Securities act	Securities and exchange commission (SEC)	Regulates the securities market, including initial public offerings (IPOs) and securities trading.
United States	Commodity exchange act	Commodity futures trading commission (CFTC)	Oversees the trading of commodity futures and options markets.
United States	Office of the comptroller of the currency (OCC)	Office of the comptroller of the currency (OCC)	Supervises national banks and federal savings associations, ensuring safe and sound operations.
European union	Fifth anti-money laundering directive (5AMLD)	European commission, European banking authority (EBA)	Enhances CDD requirements and reporting mechanisms to combat money laundering and terrorist financing.

Region	Key regulations	Regulatory bodies	Description
European union	Markets in financial instruments directive II (MiFID II)	European securities and markets authority (ESMA)	Regulates financial markets, ensuring transparency and investor protection.
European union	General data protection regulation (GDPR)	European data protection board (EDPB), national data protection authorities (DPAs)	Sets stringent guidelines on data protection and privacy, impacting how financial institutions handle customer data.
United Kingdom	Financial services and markets act 2023	Financial conduct authority (FCA), prudential regulation authority (PRA)	Replaces retained EU laws with UK-specific regulations, ensuring compliance and financial stability post-Brexit.
United Kingdom	Money laundering, terrorist financing and transfer of funds (Information on the payer) regulations 2017 (Updated 2020)	FCA, PRA	Aligns UK AML laws with international standards set by FATF, incorporating enhanced due diligence and reporting requirements.
United Kingdom	General data protection regulation (GDPR)	Information commissioner's office (ICO)	Although Brexit has led to UK GDPR, the principles remain largely consistent with EU GDPR, ensuring high standards of data protection and privacy.
United Kingdom	Payment services regulations 2017	FCA	Implements the EU's second payment services directive (PSD2), promoting competition and innovation while enhancing security in electronic payments.

## 7.2. Emerging Regulatory Trends

The evolution of FinTech services has been unprecedented and has fostered the use of dynamic and flexible regulatory systems worldwide. With FinTech becoming increasingly popular in delivering financial services, managing the associated risks has become paramount.

### 7.2.1. Digital Assets and Cryptocurrencies

With the growing use of digital assets like bitcoins, regulation is the only available option to mitigate risks and issues such as fraud, malpractice, market manipulation, and financial volatility. In the United States, distinct federal authorities such as the Security Exchange Commissions (SEC) and the Commodity Futures Trading Commission (CFTC) play a crucial role in overseeing the crypto assets category. The SEC is responsible for the securities aspect, investor protection, and overall market protection, while the CFTC regulates the derivatives and commodities segment. In the EU context, the proposed Markets in Crypto-Assets (MiCA) regulation has been designed to create a constructive legal framework for digital assets. According to [Tran and Kevin \(2023\)](#) Mica aims to offer more explicit legal specifications, propel innovation, and bolster consumer protection across member states. This regulation is also expected to reduce fragmentation in this area and provide more certainty to those who invest in digital assets.

### 7.2.2. Artificial Intelligence (AI) and Machine Learning

Adopting AI and machine learning in financial services has attracted controversy over data privacy, security, and the ethical implications of the algorithms used. Regulators are not idle; they are actively working to develop policies and standards to prevent the misuse of AI. For instance, the UK government convened the AI Safety Summit, where it was evident that the government was paying adequate attention to implementing proper regulatory measures. Most discussions focused on the transparency of AI programming, accountability for AI decision-making, and mechanisms to ensure that AI does not act in a discriminatory manner. Furthermore, the whitepaper on AI published by the UK government outlines plans to govern AI and emphasizes the need to prevent

adverse effects while fostering technological advancement (Int-Comp.org, 2023). The EU and the US also face these challenges, and their regulatory authorities are developing regulations for AI to address these issues.

### 7.2.3. Sustainable Finance

ESG has gradually become one of the key issues affecting financial regulation. The Sustainable Finance Disclosure Regulation (SFDR) applies to firms in the EU, requiring them to make sustainable investments and disclose them based on ESG factors included in the investment process. This regulation aims to enhance disclosure practices in such enterprises so that investors can make decisions based on sustainability. Furthermore, the Corporate Sustainability Due Diligence Directive (CSDDD) proposes that firms must identify and address risks of human rights violations and environmental crimes throughout the supply chain (Int-Comp.org, 2023). These are signs of a more profound transition towards integrating sustainability in financial activities due to investors' growing demand for sustainable funds.

### 7.3. Role of International Cooperation

FinTech is a facilitator of global financial crimes, and for this reason, they can only be fought through international collaboration. However, FinTech innovations also introduce risks in the form of opportunities for some of these financial crimes, as they are frequently transnational and demand an international response.

#### 7.3.1. Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF)

FATF is renowned for implementing recommendations and maintaining an international list of countries concerning AML and CTF. Money laundering is a focus of FATF, which requires countries to adopt very stringent measures to combat this vice. The Mutual Evaluations performed by FATF assess how states incorporate these standards and provide information, thus encouraging the timely ratification of best practices. These evaluations reveal a lack of measures to implement substantial norms at the national level regarding AML/CTF, thereby continuing to provide recommendations for improving norms worldwide, with the purpose of uniting to fight financial crimes (Financial Action Task Force (FATF), 2023). FATF's approach entails cooperation through which these countries work together, thereby improving best practices in the financial field and enhancing financial security globally.

#### 7.3.2. Cybersecurity

Growing cybersecurity threats present significant risks to the finance sector and thus call for global collaboration. Organizations such as the European Union Agency for Cybersecurity (ENISA) and the US Cybersecurity & Infrastructure Security Agency (CISA) facilitate the sharing of best practices and threat intelligence between nations. These organizations work to create uniform cybersecurity standards and strengthen incident response mechanisms. Facilitating international cooperation helps reduce the cyber risks experienced by financial entities worldwide. Collaborating around cybersecurity, including sharing information and orchestrating cyber-threat responses, is essential to protecting enterprises from advanced threats that can have far-reaching impacts. Joint efforts dealing with cyber risks, such as data protection of sensitive personal identities, provide critical capabilities for identifying new attack trends (McKinsey & Company, 2021a). Cyber threats are global, and no country can solve these challenges alone, emphasizing the necessity of international cooperation.

#### 7.3.3. Data Security and Privacy

The global data movement necessitates standard policies around data protection. The EU has established a high standard for data privacy with its General Data Protection Regulation (GDPR), and more governments worldwide are expected to follow suit. The goal is to enable data transfers while maintaining privacy, forming the

basis of collaborative organizations such as the EU-US Privacy Shield. This agreement allows the processing and transfer of personal data between the EU and the US while reconciling regulatory requirements with global commerce (Global Legal Insights, 2023). Streamlining data protection legislation globally safeguards individuals' privacy rights and ensures clarity for businesses operating across borders.

#### 7.3.4. Global Financial Regulation

International initiatives led by the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS), and forums like the G20 act as platforms to harmonize and discuss key financial landscape issues. These forums provide a synchronized global regulatory framework, allowing for comprehensive discussions and understanding of prudential requirements and financial reforms.

Conclusively, international collaboration is vital to tackle the nuances and challenges of financial crimes in the FinTech era. Countries need to work collaboratively and independently to develop more muscular regulatory structures, share intelligence, and execute better strategies to eradicate financial crimes, creating a secure world of finance.

## 8. WEIGHING THE BENEFITS AND RISKS

### 8.1. Benefits to Financial Institutions

#### 8.1.1. Enhanced Efficiency and Cost Reduction

FinTech solutions improve the operations of financial institutions by reducing the need for the workforce to perform various tasks. Automated systems for customer acquisition, loan processing, and compliance save time, leading to significant cost savings. For instance, automated customer verification systems allow firms to address KYC requirements much faster, completing the process in minutes rather than the days or weeks required for manual procedures. Research conducted by Accenture shows that integrating FinTech solutions can optimize operational costs by up to 30% (Accenture, 2021).

#### 8.1.2. Improved Customer Experience

Various innovations in financial technology have enhanced customer experience by adopting mobile banking apps and other online services. Customers can now manage their banking needs, conduct transactions, borrow, invest, and more, all from the comfort of their homes. This convenience increases customer satisfaction and, consequently, customer loyalty. A study by PricewaterhouseCoopers (PwC) revealed that nearly half of consumers now rely solely on digital means to access their financial services; 46% of consumers have transitioned to purely digital channels for their financial needs (PwC, 2021).

#### 8.1.3. Enhanced Fraud Detection and Security

FinTech solutions equipped with artificial intelligence (AI) and machine learning (ML) algorithms provide robust fraud detection capabilities. Systems like the ARIC Risk Hub by Feature space use adaptive behavioral analytics to detect anomalies and potential fraud in real-time. These technologies have been shown to block up to 75% of fraudulent transactions, significantly reducing financial losses and enhancing security (Sutton, 2022).

#### 8.1.4. Financial Inclusion

FinTech has played a crucial role in promoting financial inclusion by providing financial services to underserved populations. Mobile banking and microfinance platforms allow individuals in remote or underbanked regions to access financial services, thereby fostering economic growth. According to the World Bank, FinTech innovations have contributed to a 20% increase in financial inclusion in developing countries over the past decade (World Bank, 2022).

#### *8.1.5. Data-Driven Decision Making*

The vast amounts of data generated by FinTech applications enable financial institutions to make more informed decisions. Advanced data analytics tools allow banks to analyze customer behavior, market trends, and financial risks more accurately. This leads to better product offerings, personalized services, and efficient risk management. A report by McKinsey & Company highlighted that data-driven decision-making processes can increase the profitability of financial institutions by 20% (McKinsey & Company, 2021b).

#### *8.2. Risks to Financial Integrity and Strategies for Mitigating Risks*

Adopting new FinTech solutions has introduced new threats to financial stability and integrity. While innovation brings numerous benefits, it poses significant risks that must be managed effectively to ensure security and compliance.

##### *8.2.1. Cybersecurity Threats*

FinTech relies heavily on digital platforms, making financial institutions vulnerable to cyber risks. Criminals target these platforms to exploit their vulnerabilities. Data breaches, ransomware attacks, and hacking can result in substantial financial losses and damage the institution's reputation. For example, the average cost of a data breach in the financial sector was \$5.72 million in 2021 (IBM, 2021). The interconnected nature of FinTech systems exacerbates the issue, as an attack on one part can directly impact the entire system.

##### *8.2.2. Regulatory and Compliance Challenges*

Rapid innovation within the FinTech sector significantly pressures compliance. Financial institutions must navigate a complex and ever-evolving landscape of regulations. The challenge is further compounded by regional regulatory differences, particularly for institutions operating in multiple countries. Non-compliance can lead to severe fines and legal consequences. In 2021, compliance expenditures for financial institutions were estimated at \$270 billion (Deloitte, 2021). Developing and maintaining compliance frameworks requires ongoing investment and adaptation to regulatory changes.

##### *8.2.3. Increased Fraud and Money Laundering*

The flexibility offered by digital transactions and cryptocurrencies can facilitate fraud and money laundering. According to the European Union Agency for Cybersecurity (ENISA), there was a 50% increase in financial crimes involving cryptocurrencies within a year (ENISA, 2022). Criminals exploit gaps in digital identity management to create fake identities, leading to significant financial losses for institutions and customers.

##### *8.2.4. Technological Dependence and System Failures*

Heavy reliance on technology introduces risks related to system failures and technological disruptions. Technical glitches, software bugs, or failures in third-party services can disrupt operations, leading to financial losses and customer dissatisfaction. For instance, the 2021 outage of the payment processing service Fastly disrupted numerous financial services globally (McKinsey & Company, 2021a). This dependence necessitates robust disaster recovery and continuity planning.

##### *8.2.5. Privacy and Data Protection Concerns*

FinTech's use of large volumes of sensitive customer data raises significant privacy and data protection concerns. Compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) in the EU, is crucial to avoid legal repercussions and maintain customer trust. Data breaches not only result in



financial losses but also lead to severe reputational damage. According to the World Economic Forum, 58% of data breaches in the financial sector involve insider threats, emphasizing the need for stringent data protection measures (World Economic Forum, 2022).

The only way to counteract these threats with any hope of success is through financial institutions' heavy investment in cybersecurity measures. This involves leveraging high-level encryption, two-factor authentication, and real-time network monitoring. Partnering with cybersecurity companies and joining intelligence-sharing efforts can give institutions an upper hand on new threats. By implementing AI-powered security systems, organizations are better equipped to detect and respond to threats quickly, creating an added level of defense.

Table 3 provides an overview of the potential FinTech-related risks, their effects, and strategies for mitigating the risks.

**Table 3.** Risks and strategies for mitigating risks.

Risk	Impact	Mitigation strategies
Cybersecurity threats	Data breaches, ransomware attacks, financial losses, reputational damage	Implement advanced encryption, multi-factor authentication, continuous network monitoring, collaborate with cybersecurity firms, participate in information-sharing initiatives (IBM, 2021).
Regulatory and compliance challenges	Hefty fines, legal repercussions, operational disruptions	Establish dedicated compliance teams, engage with regulators, invest in RegTech solutions, monitor regulatory changes, participate in industry forums (Deloitte, 2021).
Increased fraud and money laundering	Financial losses, reputational damage, regulatory fines	Adopt AI and ML-based fraud detection systems, implement stringent KYC and AML protocols, conduct regular audits and assessments (ENISA, 2022).
Technological dependence	System failures, operational disruptions, financial losses, customer dissatisfaction	Develop comprehensive disaster recovery and business continuity plans, invest in resilient IT infrastructure, conduct regular drills and simulations (McKinsey & Company, 2021a).
Privacy and data protection concerns	Legal repercussions, financial losses, reputational damage	Comply with data protection regulations (e.g., GDPR), implement stringent data protection measures, conduct regular audits and assessments, promote a culture of data security (World Economic Forum, 2022).

Another critical factor in risk management is compliance. Banks should hire compliance officers to monitor regulations and implement changes immediately. This approach makes it easier for institutions to remain compliant and to understand potential issues from regulators shortly. Using technology solutions in compliance, such as RegTechs, is another way to address non-compliance risk, as some processes can be automated.

The elements of the right balance for success in IoT depend heavily on the capacity of financial institutions to combat fraud and money laundering. Systems that can detect deviations from typical transactions in real-time play a crucial role in fraud prevention. However, it's the comprehensive audits and assessments that truly increase awareness of weaknesses, providing necessary checks for a secure institution and ensuring the institution is ready to combat fraud and money laundering.

Disasters caused by technological disruptions are devastating and should be addressed by recovery and continuity management. Backup, redundancy, and crisis management strategies should also be part of the essential plans. Banks should train through drills and simulations to ensure they are prepared to respond to calamities in various scenarios. Methods such as establishing a robust information technology framework and relying on cloud services assist in improving dependability, thereby minimizing the disruptive effects on activities.

Financial marketing and customer education can also be beneficial. Teaching customers responsible behaviors and how to protect themselves while conducting transactions via digital financial services will significantly minimize the risk of fraud. Financial institutions must offer resources and tools to help customers recognize

suspicious activities, such as mule accounts, and proactively stay informed on ways to protect themselves against future financial crimes. This approach enhances security and builds customer trust and confidence in digital financial services.

## 9. FUTURE OUTLOOK

### 9.1. *Emerging Technologies and Trends*

The International Monetary Fund (IMF) is focusing on utilizing distributed ledger technology to leverage FinTech for cross-border payments; augmented reality to improve customer satisfaction is one of the rising themes. Digital invoicing, digital insurance, crowdsourcing, investing in crowds, robotics investment advising, The regulatory function of central banks and their future connections with FinTech companies (Pant, 2020). Emerging trends include the use of mobile wallets, the rise of virtualized neo-banks, and the increased interaction of millennial consumers with internet giants like Google and Amazon. These companies have used blockchain for peer-to-peer lending and contract administration, artificial intelligence for investment advice, machine learning and data analytics for customer service, etc. Augmented Reality (AR) has the potential to significantly differentiate services from one another and improve client engagement. With AR, users may view information in a clear, simple, and immersive manner (Dubey, 2019). FinTech companies employ a variety of significant technologies in their product development processes, including blockchain, machine learning, artificial intelligence, data analytics, robots, and cloud computing. According to an evidence-based analysis, the three most beneficial breakthroughs for the financial sector are blockchain, robo-advising, and the Internet of Things (IoT) (Chen, Wu, & Yang, 2019). Unmanned aerial vehicles have been used in the insurance, financial, and underwriting domains employing sensor data collection and wireless transmission to adjust insurance claims (Luciani, Distasio, Bungert, Sumner, & Bozzo, 2016). China and India are the world's leaders in the adoption and awareness of digital payments. It is now the foundation of many non-financial businesses, including Fast-moving consumer goods (FMCG) (point of sale), e-commerce, insurance (comparison, purchase), telecom & utility (recharges, bill payments), travel (bookings, payments, offers), hospitality (booking, payments), entertainment (content purchases), and FMCG (travel). Even in many nations, such as India, the government transfers funds directly for purchases and subsidies to cut down on corruption and save transaction costs. With more innovation, digital payments will remain a fundamental component of FinTech services (Pant, 2020). Robotic advisors and chatbots are perceived as ways to assist clients that human advisors cannot. For example, unlike human advisors, robo-advisers often use technology that may simplify and expedite client communication, apply repeatable algorithms based on financial theory, and are far more transparent (D'Acunto, Prabhala, & Rossi, 2019). One cannot isolate the application of Big Data, AI, and machine learning from emerging technological advancements in the FinTech industry. The impact of using data is wide-ranging and complex, which is why this sector is so concerned about data security. In this setting, data security is just as important as technical security. FinTech must safeguard customers from problems with data breaches and limitations on data access, including the security of personal data. Therefore, it is necessary to have rigorous regulations about the security of personal data. Digital literacy is another thing that consumers need to know. Cyberliteracy necessitates careful technology users. To prevent fraud, the FinTech sector must also preserve the calibre of its software and make use of technological integration (Hua, Huang, & Zheng, 2019). At the moment, FinTech companies must work together with more established financial institutions like banks. This tackles the issue that FinTech is a disruptive technological advancement. Because FinTech is thought to follow digital transformation more quickly than other companies, banks need to work with them as strategic partners (Fermay, Santosa, Kertopati, & Eprianto, 2018).

### 9.2. *Predictions for Financial Crime Landscape*

With a few notable exceptions, including mortgage fraud, practically all fraud categories have experienced significant rises. The quantity of external fraud has increased, as has the volume of transactions overall (Kurshan,

Shen, & Yu, 2020). Fraud involving payments includes transactions using credit and debit cards, automated clearing houses (ACH), wire transfers, person-to-person (P2P) transactions, online payments, automated bill payments, cheques, and deposits, among other payment channels. Across all payment channels, fraud has increased significantly in recent years, with digital transactions seeing the largest rise (Dorphy & Hultquist, 2018). A variety of strategies, such as ATM skimming devices, phishing, smishing, dumpster diving, and infiltrated wireless networks, are employed by identity theft schemes. Identity theft is becoming one of the most common forms of fraud reported in criminal files made to the Federal Trade Commission (Kurshan et al., 2020). One of the main issues in the fraud environment these days is financial frauds. These crimes employ ever-evolving strategies, including scams using phones, elderly victims (like grandmother scams), tech support scams, scams involving charities and lotteries, scams involving tickets, etc (Spreng, Ebner, Levin, & Turner, 2021). When thieves obtain unauthorized access to a victim's account, account takeover fraud takes place. To prevent the victim from accessing the account, thieves usually alter the contact details and account login passwords throughout this procedure. Eventually, they use one or more payment channels to drain the cash. Australian Taxation Office (ATO) is closely related to cybersecurity because of the frequent use of hacked devices and networks, SIM hijacking, and large-scale data breaches as means of attack (Gies, Piquero, Piquero, Green, & Bobnis, 2021). The capacity to quickly adjust to new trends, weaknesses, and preventative measures is demonstrated by crime techniques.

They utilize cross-channel strategies in addition to demonstrating astounding degrees of personalization to the specific channels they use. In terms of transaction type (amounts, processing times), channel, devices, authentication requirements, etc., there are noticeable variations in fraud characteristics. Because of this, automated teller machine (ATM) fraud differs greatly from online bill payment fraud in several ways, including frequency, quantities, transaction and processing time spans, parties involved, compromised access, and devices involved (Kurshan et al., 2020).

## 10. CONCLUSION

### 10.1. Summary of Findings

The goal of the paper is to evaluate FinTech's impact and to analyze whether it is a curse or blessing for financial institutions. The paper discusses the landscape of the FinTech historical context and current trends, overview, classification, methods and mechanism of financial crimes, and the impact of those crimes on financial institutions, government, economy and consumers. Positive impacts of FinTech on financial crime prevention also have been discussed including the cases of successful implementation.

The findings of the paper show that FinTech is acknowledged as the most cutting-edge innovation in the financial sector for improving quality, lowering costs, and expanding an efficient financial environment. Several drivers of transformation brought about by IT have a big impact. Through automation, new models such as peer-to-peer investing and crowdfunding boost information technology efficiency and guarantee the quality of financial services. Blockchain-based systems and biometrics (such as fingerprints, face recognition, and iris scans) are examples of new technologies that can enhance digital identification procedures. By providing improved security, decreased fraud, and expedited identification verification processes, these technologies help stop theft and other associated crimes. Systems for monitoring finances can benefit from the application of artificial intelligence, machine learning, and advanced data analytics. These technological advancements facilitate the prompt and precise detection of dubious transactions, money laundering operations, and fiscal offenses. Automated systems can analyze enormous volumes of data and spot trends that are hard for people to see, which helps law enforcement fight financial crimes. To guarantee successful adoption and adherence to international standards as these technologies advance, regulatory agencies, financial institutions, and technology suppliers must work together. This will eventually help to create a more robust and safer financial environment. Big data's ascent has revolutionized fraud detection and financial security by offering previously unheard-of analytical powers. Financial institutions are increasingly able to

expose sophisticated fraud schemes through the use of large datasets. These schemes can involve everything from money laundering and complicated securities fraud to improper credit card transactions and insurance fraud. Additionally, by utilizing hybrid client contact, the expansion of the customer base significantly contributes to the resizing of the channel management route to clients. A new competition by FinTech companies causes existing challenges, faced by the traditional banking environment. The convergence between emerging business models and technology improves streamlined operations and customer satisfaction. A digital finance cube is innovated with the consensus of business operations, technologies and technological concepts which has significant influence over various stakeholders from three dimensions (consumers, market players and regulatory font).

### *10.2. Final Verdict: Curse or Blessing?*

The effectiveness of cloud-based finance apps to prevent fraud is greatly influenced by AI. Machine learning algorithms have the capability to process vast datasets and detect patterns associated with fraudulent activities such as credit card fraud, identity theft, and account takeovers. AI systems continuously learn from new data, which helps them become more adept at spotting novel fraud techniques. FinTech companies utilize an array of emerging technologies, including big data, IoT, blockchain, robotics, augmented reality, artificial intelligence, robotics, and drones. As a major international financial organization, the International Monetary Fund (IMF) thinks that blockchain distributed ledger technology might help FinTech companies increase cross-border payment services, transaction costs, and transparency.

More study may be done on the more recent subjects of digital insurance, digital invoicing, electronic factoring, electronic leasing, crowd investing, and the connections between cryptocurrencies other than bitcoin. Robotic financial advice has the potential to upend the investment consulting industry. These robo-advisors are more affordable, provide more educated information, and satisfy client expectations for trust and openness (Pant, 2020). Blockchain has the power to completely change industries, save money, and increase openness and trust in company operations. One of blockchain's most potent features is its ability to track any transaction from source to target with reliable middlemen. This has many applications, including tracking diamonds from mine to retail establishments, organic farming from farmer to market, land records for transparent ownership history, and sharing patient medical records.

The extraordinary rise in digital payments in recent years has led to significant shifts in financial crimes and fraud. In contrast to the growing reliance on complex digitalized information technology hubs without replacement, FinTech is becoming increasingly visible from the outside, increasing cyber exposure. Cybercriminals may utilize these security flaws to hijack equipment supporting the financial system, disrupt payment systems, or access data at custodian banks or Central Securities Depositories (Buckley et al., 2019). With the growing use of digital payments, there is a greater chance of financial fraud. Consequently, NPSs—which are directly controlled by Central Banks (CBs)—are increasingly utilizing state-of-the-art technologies, such cognitive computing, to enhance their ability to detect fraud inside their countries (Alessio Faccia, 2023).

After thorough analyses of both the positive and negative implications of FinTech, we can conclude that for every disruptive technology, there are some drawbacks along with the benefits. However, by capitalizing the emerging technologies we can tackle the problems. Experiments in the real world, such as the Financial Crimes Section of the FBI's detection and disruption of large-scale fraud schemes, show how important machine learning and big data are to protecting the nation's financial borders (Saxena & Vafin, 2019). Solutions based on graph computing concepts for AI and machine learning have attracted a lot of attention. Graph neural networks and newly developed adaptive solutions provide promising prospects for the identification of financial crimes and fraud in the future.

## 11. IMPLICATIONS

Our paper provides insights into both the positive and negative impact of FinTech on financial institutions, the economy and consumers that contribute to both practical and theoretical implications. Financial institutions will be more aware of the different kinds of crimes and related crimes generated by employing FinTech. Future researchers can add more knowledge by suggesting and finding out how emerging crimes can be mitigated. The following are some ways that trade and investment implementing authorities can help the FinTech Pod succeed: assigning FinTech experts to oversee FinTech Bridge initiatives, such as offering customized strategic counsel to FinTech companies establishing operations in a State Party; acting as a point of contact for FinTech companies in each market, offering support with inquiries and opportunity identification; establishing connections amongst FinTech personnel employed by appropriate trade and investment implementing authorities; assisting in matching events, gatherings, and networking chances for businesses interested in partnering. Like scammers always come up with new methods to trick financial institutions, FinTech is changing as a result of the emergence of cutting-edge technology that employ AI to stop and identify fraud. Detecting and preventing fraud is a continuous process. In the FinTech industry, fraud may be prevented and detected with the use of contemporary technology like AI and machine learning. At the corporate, managerial, and personal levels, integrity and ethical concerns with fintech would presumably never go away. It is crucial to remember that cybersecurity education and training would be ineffective if it didn't address the fraud concerns related to human ethics and integrity. For the Fintech experts working on the overall architecture and growth of the Fintech infrastructure, such moral behaviour is even more important.

**Funding:** This study received no specific financial support.

**Institutional Review Board Statement:** Not applicable.

**Transparency:** The authors declare that the manuscript is honest, truthful and transparent, that no important aspects of the study have been omitted and that all deviations from the planned study have been made clear. This study followed all rules of writing ethics.

**Data Availability Statement:** The corresponding author can provide the supporting data of this study upon a reasonable request.

**Competing Interests:** The authors declare that they have no competing interests.

**Authors' Contributions:** All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

## REFERENCES

- Abdul-Qawy, A. S., Pramod, P., Magesh, E., & Srinivasulu, T. (2015). The internet of things (IOT): An overview. *International Journal of Engineering Research and Applications*, 5(12), 71-82.
- Accenture. (2016). *Global FinTech investment growth continues in 2016 driven by Europe and Asia, Accenture study find*. Retrieved from <https://www.accenture.com/us-en>
- Accenture. (2021). *Cost reduction in financial services through FinTech*. Retrieved from <https://www.accenture.com/in-en>
- Achim, M. V., & Borlea, S. N. (2020). *Economic and financial crime*: Springer International Publishing. <https://doi.org/10.1007/978-3-030-51780-9>.
- Achim, M. V., Pisoni, G., Mare, C., Moloney, M., Korba, S., Molnár, B., . . . Coita, I. F. (2023). FinTech, regulation, and cybercrime: Opportunities arising from new technologies. *Available at SSRN*. <https://doi.org/10.2139/ssrn.4620106>
- Adeosun, O. A., Anagreh, S., Tabash, M. I., & Adedokun, A. (2023). Revisiting the connectedness between oil prices and uncertainty indicators in BRICS countries. *Resources Policy*, 86, 104278. <https://doi.org/10.1016/j.resourpol.2023.104278>
- Alade, I. (2023). Reconceptualization of corporate governance for fintech firms. *Loyola of Los Angeles International and Comparative Law Review (Forthcoming)*.
- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, 563060. <https://doi.org/10.3389/fcomp.2021.563060>



- Amadi, A. (2023). Integration in a mixed-method case study of construction phenomena: From data to theory. *Engineering, Construction and Architectural Management*, 30(1), 210-237.
- Anagnostopoulos, I. (2018). FinTech and regtech: Impact on regulators and banks. *Journal of Economics and Business*, 100, 7-25. <https://doi.org/10.1016/j.jeconbus.2018.07.003>
- Antal, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I. (2021). Distributed ledger technology review and decentralized applications development guidelines. *Future Internet*, 13(3), 62. <https://doi.org/10.3390/fi13030062>
- Arner, D. W., Barberis, J., & Buckley, R. P. (2016). FinTech, RegTech, and the reconceptualization of financial regulation. *Journal of International Law and Business*, 37, 371.
- Arner, D. W., Barberis, J., & Buckley, R. P. (2015). The evolution of fintech: A new post-crisis paradigm. *Georgetown Journal of International Law*, 47, 1271.
- Barefoot, J. A. (2020). Digital technology risks for finance: Dangers embedded in fintech and regtech. *M-RCBG Associate Working Paper Series*, 151.
- Barr, M., Gifford, K., & Klein, A. (2018). Enhancing anti-money laundering and financial access: Can new technology achieve both?
- Bartlett, B. L. (2002). *The negative effects of money laundering on economic development*. Asian Development Bank Regional Technical Assistance Project No, 5967.
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. V. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 471-482. <https://doi.org/10.25300/misq/2013/37:2.3>
- Bhasin, M. L. (2016). Accounting manipulations in corporate financial reports: Study of an Asian market. *International Journal of Management Sciences and Business Research*, 1-5(11), 24.
- Bhattacharya, U., & Daouk, H. (2002). The world price of insider trading. *The Journal of Finance*, 57(1), 75-108.
- Bin Azero, M. A., Abdullah, S. N. A. K., Zakaria, Z., Haris, H., Yusoff, Y. H., & Alam, P. (2024). The nexus of cybercrime and money laundering: A conceptual paper. *Accounting and Finance Research*, 13(2), 167-167. <https://doi.org/10.5430/afr.v13n2p167>
- Boles, J. R. (2017). Million dollar ghost buildings: Dirty money flowing through luxury real estate markets.
- Borgogno, O., & Colangelo, G. (2020). Consumer inertia and competition-sensitive data governance: The case of open banking. *Journal of European Consumer and Market Law*, 9, 143.
- Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems*, 56, 684-700.
- Buckley, R. P., Arner, D. W., Zetsche, D. A., & Selga, E. (2019). The dark side of digital financial transformation: The new risks of fintech and the rise of techRisk. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3478640>
- Chan, R., Troshani, I., Rao Hill, S., & Hoffmann, A. (2022). Towards an understanding of consumers' FinTech adoption: The case of open banking. *International Journal of Bank Marketing*, 40(4), 886-917. <https://doi.org/10.1108/ijbm-08-2021-0397>
- Chang, J. J., Lu, H. C., & Chen, M. (2005). Organized crime or individual crime? Endogenous size of a criminal organization and the optimal law enforcement. *Economic Inquiry*, 43(3), 661-675. <https://doi.org/10.1093/ei/cbi046>
- Chen, L. d. (2008). A model of consumer acceptance of mobile payment. *International Journal of Mobile Communications*, 6(1), 32-52.
- Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, 19, 171-209.
- Chen, M. A., Wu, Q., & Yang, B. (2019). How valuable is FinTech innovation? *The Review of Financial Studies*, 32(5), 2062-2106.
- Chen, X., Teng, L., & Chen, W. (2022). How does FinTech affect the development of the digital economy? Evidence from China. *The North American Journal of Economics and Finance*, 61, 101697.
- Chinnasamy, G., Madbouly, A., & Reyad, S. (2021). Fintech: A pathway for MENA region. *The Fourth Industrial Revolution: Implementation of Artificial Intelligence for Growing Business Success*, 135-151.

- Chorvatovičová, L., & Saxunová, D. (2016). *Usefulness of financial statements and annual reports in the process of accounting fraud detection*. Paper presented at the In Managing Global Changes: Proceedings of the Joint International Conference. pp. 233-247.
- Christie, R. M. (1969). *A study in criminal theory with special reference to white collar crime*. Doctoral Dissertation, University of London, Bedford College (United Kingdom).
- Crockett, A. (1996). The theory and practice of financial stability. *De Economist*, 144(4), 531-568.
- D'Acunto, F., Prabhala, N., & Rossi, A. G. (2019). The promises and pitfalls of robo-advising. *The Review of Financial Studies*, 32(5), 1983-2020.
- Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research. *Electronic Commerce Research and Applications*, 14(5), 265-284. <https://doi.org/10.1016/j.eierap.2015.07.006>
- Daofu, C. H. E. N. (2020). Reflections on Fintech and regulatory measures in China. *China Economic Transition= Dangdai Zhongguo Jingji Zhuanxing Yanjiu*, 3(2), 30-44.
- De Prado, M. L. (2018). *Advances in financial machine learning*. New Jersey: John Wiley & Sons.
- Deloitte. (2021). *Global compliance spending in financial services*. Retrieved from <https://www.deloitte.com/bd/en.html>
- Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and cyber security in FinTech. In Digital transformation of the financial industry: Approaches and applications. In (pp. 255-272). Cham: Springer International Publishing.
- Dhali, M., Hassan, S., Mehar, S. M., Shahzad, K., & Zaman, F. (2023). Cryptocurrency in the darknet: Sustainability of the current national legislation. *International Journal of Law and Management*, 65(3), 261-282. <https://doi.org/10.1108/IJLMA-09-2022-0206>
- Dorphy, A., & Hultquist, H. (2018). 2017 financial institution payments fraud mitigation survey. *Federal Reserve Bank of Minneapolis*.
- Dubey, V. (2019). FinTech innovations in digital banking. *International Journal of Engineering Research & Technology*, 8(10), 597-601. <https://doi.org/10.17577/ijertv8is100285>
- Duran, R. E., & Griffin, P. (2021). Smart contracts: Will Fintech be the catalyst for the next global financial crisis? *Journal of Financial Regulation and Compliance*, 29(1), 104-122. <https://doi.org/10.1108/jfrc-09-2018-0122>
- ENISA. (2022). *Threat landscape report 2022*. Retrieved from [https://european-union.europa.eu/index\\_en](https://european-union.europa.eu/index_en)
- Faccia, A. (2023). National payment switches and the power of cognitive computing against fintech fraud. *Big Data and Cognitive Computing*, 7(2), 76. <https://doi.org/10.3390/bdcc7020076>
- Faccia, A., Moşteanu, N. R., Cavaliere, L. P. L., & Mataruna-Dos-Santos, L. J. (2020). *Electronic money laundering, the dark side of FinTech: An overview of the most recent cases*. Paper presented at the In Proceedings of the 2020 12th International Conference on Information Management and Engineering (pp. 29-34).
- Fermay, A. H., Santosa, B., Kertopati, A. Y., & Eprianto, I. M. (2018). *The development of collaborative model between FinTech and bank in Indonesia*. Paper presented at the In Proceedings of the 2nd International Conference on E-Commerce, E-Business and E-Government. pp. 1-6.
- Fernandez-Vazquez, S., Rosillo, R., De La Fuente, D., & Priore, P. (2019). Blockchain in FinTech: A mapping study. *Sustainability*, 11(22), 6366. <https://doi.org/10.3390/su11226366>
- Financial Action Task Force (FATF). (2023). *The FATF recommendations*. Retrieved from <https://www.fatf-gafi.org/>
- Financial Crisis Inquiry Commission. (2011). *The financial crisis Inquiry report: The final report of the national commission on the causes of the financial and economic crisis in the united states, including dissenting views*: Cosimo, Inc.
- Fisman, R., & Svensson, J. (2007). Are corruption and taxation really harmful to growth? Firm level evidence. *Journal of Development Economics*, 83(1), 63-75. <https://doi.org/10.1016/j.jdevec.2005.09.009>
- Fong, D., Han, F., Liu, L., Qu, J., & Shek, A. (2021). Seven technologies shaping the future of fintech. *McKinsey Analysis November*, 9.
- Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. *Journal of Network and Computer Applications*, 103, 262-273. <https://doi.org/10.1016/j.jnca.2017.10.011>

- Gelb, A. H. (1989). *Financial policies, growth and efficiency policy planning and research*. Working Papers, No. 202, World Bank.
- Ghazali, N. H., & Yasuoka, T. (2018). Awareness and perception analysis of small medium enterprise and start-up towards fintech instruments: Crowdfunding and peer-to-peer lending in Malaysia. *International Journal of Finance and Banking Research*, 4(1), 13-24. <https://doi.org/10.11648/j.ijfbr.20180401.12>
- Gies, S. V., Piquero, N. L., Piquero, A. R., Green, B., & Bobnis, A. (2021). Wild, wild theft: Identity crimes in the digital frontier. *Criminal Justice Policy Review*, 32(6), 592-617. <https://doi.org/10.1177/0887403420949650>
- Giudici, P. (2018). Fintech risk management: A research challenge for artificial intelligence in finance. *Frontiers in Artificial Intelligence*, 1, 1. <https://doi.org/10.3389/frai.2018.00001>
- Global Legal Insights. (2023). *FinTech laws and regulations*. Retrieved from <https://www.globallegalinsights.com/practice-areas/FinTech-laws-and-regulations/>
- Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). Financial information systems and the fintech revolution. *Taylor & Francis*, 35(1), 12-18.
- Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital finance and FinTech: Current research and future research directions. *Journal of Business Economics*, 87, 537-580. <https://doi.org/10.1007/s11573-017-0852-x>
- Goni, O., & Alam, M. M. (2022). The basic concept of cyber crime and criminal. *International Journal of Electronics and Information Engineering*, 14(1), 39-54.
- Gopalan, S., Jain, G., Kalani, G., & Tan, J. (2012). Breakthrough IT banking. *McKinsey Q*, 26, 30-35.
- Gottschalk, P. (2010). Theories of financial crime. *Journal of Financial Crime*, 17(2), 210-222. <https://doi.org/10.1108/13590791011033908>
- GOV.UK. (2023). *A smarter regulatory framework for financial services*. Retrieved from <https://www.gov.uk/government/collections/a-smarter-regulatory-framework-for-financial-services>
- Gozman, D., Liebenau, J., & Mangan, J. (2018). The innovation mechanisms of fintech start-ups: Insights from SWIFT's innotribe competition. *Journal of Management Information Systems*, 35(1), 145-179. <https://doi.org/10.1080/07421222.2018.1440768>
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660. <https://doi.org/10.1016/j.future.2013.01.010>
- Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67, 247-267. <https://doi.org/10.1007/s11235-017-0334-z>
- Gupta, S., Raj, S., Gupta, S., & Sharma, A. (2023). Prioritising crowdfunding benefits: A fuzzy-AHP approach. *Quality & Quantity*, 57(1), 379-403.
- Han, J., Huang, S., & Zhong, Z. (2023). Trust in defi: An empirical study of the decentralized exchange. *Available at SSRN* 3896461. <https://doi.org/10.2139/ssrn.3896461>
- Hansen, L. L. (2009). Corporate financial crime: Social diagnosis and treatment. *Journal of Financial Crime*, 16(1), 28-40.
- Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. *McKinsey & Company*, 2019.
- Hayashi, Y. (2016). CFPB fines FinTech firm Dwolla over data-security practices. *The Wall Street Journal*, 4.
- Hochstein, M. (2015). *FinTech (The word, that is) Evolves*. *American banker*. Retrieved from <https://www.americanbanker.com/opinion/FinTech-the-word-that-is-evolves>
- Holland FinTech. (2015). *The future of finance: The socialization of finance*. Retrieved from <http://hollandFinTech.com/the-future-of-finance-the-socialization-of-finance/>
- Hollanders, M. (2020). FinTech and financial inclusion: Opportunities and challenges. *Journal of Payments Strategy & Systems*, 14(4), 315-325. <https://doi.org/10.69554/sdin1936>
- Home of FinTech & Banking News. (2021). *The dark web and its role in financial crimes*. Retrieved from <https://fintechmagazine.com/>
- Hua, X., Huang, Y., & Zheng, Y. (2019). Current practices, new insights, and emerging trends of financial technologies. *Industrial Management & Data Systems*, 119(7), 1401-1410. <https://doi.org/10.1108/IMDS-08-2019-0431>

- IBM. (2021). *Cost of a data breach report*. Retrieved from <https://www.ibm.com/downloads/cas/JDALZGKJ>
- Int-Comp.org. (2023). *Top trends that shaped the global regulatory and financial crime compliance landscape in 2023*. Retrieved from <https://www.int-comp.org/>
- Jain, R., Prajapati, D., & Dangi, A. (2023). Transforming the financial sector: A review of recent advancements in FinTech. *Available at SSRN 4380348*.
- Karpoff, J. M., Lee, D. S., & Martin, G. S. (2008). The consequences to managers for cooking the books. *Journal of Financial Economics*, 88(88), 193-215.
- Koistinen, K. (2023). Automation of investment advisory services: Exploring the landscape of robo-advisors.
- Korejo, M. S., Rajamanickam, R., & Said, M. H. M. (2021). The concept of money laundering: A quest for legal definition. *Journal of Money Laundering Control*, 24(4), 725-736. <https://doi.org/10.1108/jmlc-05-2020-0045>
- Koskipää, S. (2022). Software development in the FinTech industry: A literature review.
- KPMG. (2015). *H2 ventures KPMG FinTech 100: Announcing the world's leading FinTech innovators for 2015*. Retrieved from <https://home.kpmg.com/xx/en/home/insights/2015/12/ventures-kpmg-FinTech-fs.html>
- Kulkarni, S. (2023). *Machine-learning-assisted recommendation system for financial organizations*. Westcliff University. <https://doi.org/10.4018/979-8-3693-5593-0.ch017>.
- Kunduru, A. R. (2023). Artificial intelligence advantages in cloud Fintech application security. *Central Asian Journal of Mathematical Theory and Computer Sciences*, 4(8), 48-53.
- Kurshan, E., Shen, H., & Yu, H. (2020). *Financial crime & fraud detection using graph computing: Application considerations & outlook*. Paper presented at the In 2020 Second International Conference on Transdisciplinary AI (TransAI) (pp. 125-130). IEEE.
- Lăzăroiu, G., Bogdan, M., Geamănu, M., Hurloiu, L., Luminița, L., & Ștefănescu, R. (2023). Artificial intelligence algorithms and cloud computing technologies in blockchain-based fintech management. *Oeconomia Copernicana*, 14(3), 707-730. <https://doi.org/10.24136/oc.2023.021>
- Le, T. T., Mai, H. N., Phan, D. T., Nguyen, M. N., & Le, H. D. (2021). FinTech innovations: The impact of mobile banking apps on bank performance in Vietnam. *International Journal of Research and Review*, 8(4), 391-401.
- Lechman, E., & Marszk, A. (2021). *The digital disruption of financial services*. Oxford: Routledge.
- Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, 61(1), 35-46. <https://doi.org/10.1016/j.bushor.2017.09.003>
- Lehmann, M. (2020). Global rules for a global market place?-Regulation and supervision of Fintech providers. *BU Int'l LJ*, 38, 118.
- Levi, M. (2015). *Foreword: Some reflections on the evolution of economic and financial crimes research handbook on international financial crime; Rider, B., Ed.* Cheltenham, UK: Edward Elgar Publishing Limited.
- Li, G., Elahi, E., & Zhao, L. (2022). Fintech, bank risk-taking, and risk-warning for commercial banks in the era of digital technology. *Frontiers in Psychology*, 13, 934053. <https://doi.org/10.3389/fpsyg.2022.934053>
- Lieonov, S. V., Bozhenko, V. V., & Mynenko, S. V. (2023). Promoting public integrity and combating financial crime: Challenges on the pathway to sustainable development.
- Loughman, B. P., & Sibery, R. A. (2011). *Bribery and corruption: Navigating the global risks*. Hoboken, NJ: John Wiley & Sons.
- Luciani, T. C., Distasio, B. A., Bungert, J., Sumner, M., & Bozzo, T. L. (2016). *Use of drones to assist with insurance, financial and underwriting related activities*, March 3 2016. US Patent App, 14(843,455).
- Macchiavello, E., & Siri, M. (2022). Sustainable finance and fintech: Can technology contribute to achieving environmental goals? A preliminary assessment of 'green fintech' and 'sustainable digital finance'. *European Company and Financial Law Review*, 19(1), 128-174. <https://doi.org/10.1515/ecfr-2022-0005>
- Mah, D. N.-Y. (2020). Conceptualising government-market dynamics in socio-technical energy transitions: A comparative case study of smart grid developments in China and Japan. *Geoforum*, 108, 148-168.

- Marqués, J. M., Ávila, F., Rodríguez-Martínez, A., Morales-Reséndiz, R., Marcos, A., Godoy, T., . . . Blanco, C. (2021). Policy report on FinTech data gaps. *Latin American Journal of Central Banking*, 2(3), 100037. <https://doi.org/10.1016/j.latcb.2021.100037>
- Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, 51(1), 176–189.
- Mascarenhas, A. B., Perpétuo, C. K., Barrote, E. B., & Perides, M. P. (2021). The influence of perceptions of risks and benefits on the continuity of use of fintech services. *BBR. Brazilian Business Review*, 18, 1–21. <https://doi.org/10.15728/bbr.2021.18.1.1>
- Matt, C., Hess, T., & Benlian, A. (2015). Digital transformation strategies. *Business & Information Systems Engineering*, 57, 339–343.
- McKinsey & Company. (2021a). *Financial crime and fraud in the age of cybersecurity*. Retrieved from <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/Risk/Our%20Insights/Financial%20crime%20and%20fraud%20in%20the%20age%20of%20cybersecurity/Financial-crime-and-fraud-in-the-age-of-cybersecurity.pdf#:~:text=URL%3A%20https%3A%2F%2Fwww.mckinsey.com%2F~%2Fmedia%2FMcKinsey%2FBusiness%2520Functions%2FRisk%2FOur%2520Insights%2FFinancial%2520crime%2520and%2520fraud%2520in%2520the%2520age%2520of%2520cybersecurity%2FFinancial>
- McKinsey & Company. (2021b). *Financial crime risk management in digital payments*. Retrieved from <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/managing-financial-crime-risk-in-digital-payments>
- Medhi, D., Singh, P., Goswami, H., & Singh, J. (2024). Futuristic approach of forensic fraud investigation in money embezzlement, asset misappropriation and larceny. *Educational Administration: Theory and Practice*, 30(6), 1283–1303.
- Mehrban, S., Nadeem, M. W., Hussain, M., Ahmed, M. M., Hakeem, O., Saqib, S., . . . Khan, M. A. (2020). Towards secure FinTech: A survey, taxonomy, and open research challenges. *IEEE Access*, 8, 23391–23406.
- Mention, A. L. (2019). The future of FinTech. *Research-Technology Management*, 62(4), 59–63.
- Mnoghithnei, I., Scorer, S., & Shingala, K. (2019). Embracing the promise of fintech. *Bank of England Quarterly Bulletin*.
- Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, 17, 1–24.
- Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International Review of Financial Analysis*, 81, 102103. <https://doi.org/10.1016/j.irfa.2022.102103>
- Mustyala, A. (2023). Leveraging blockchain for fraud risk reduction in fintech: Infrastructure setup and migration strategies. *EPH-International Journal of Science and Engineering*, 9(2), 1–10.
- Navaretti, G. B., Calzolari, G., Mansilla-Fernandez, J. M., & Pozzolo, A. F. (2018). Fintech and banking. *Friends or Foes*.
- Nelaturu, K., Du, H., & Le, D.-P. (2022). A review of blockchain in fintech: Taxonomy, challenges, and future directions. *Cryptography*, 6(2), 18.
- Nguyen, Q. K. (2022). The effect of FinTech development on financial stability in an emerging market: The role of market discipline. *Research in Globalization*, 5, 100105. <https://doi.org/10.1016/j.resglo.2022.100105>
- Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access*, 9, 163965–163986. <https://doi.org/10.1109/access.2021.3134076>
- Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, 33, 200908. <https://doi.org/10.1016/j.fsidi.2020.200908>
- Noul, U., & Hussain, R. (2024). Innovative FinTech security: Federated learning and anomaly detection techniques. *Unpublished*. <https://doi.org/10.13140/RG.2.2.17108.62083>



- Nüesch, R., Alt, R., & Puschmann, T. (2015). Hybrid customer interaction. *Business & Information Systems Engineering*, 57, 73-78. <https://doi.org/10.1007/s12599-014-0366-9>
- NVIDIA. (2022). *Featurespace blocks fraud attacks for financial institutions with AI and NVIDIA GPUs*. Retrieved from <https://blogs.nvidia.com/blog/featurespace-blocks-financial-fraud/>
- O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *LET Networks*, 7(5), 321-327.
- Okunleye, O. (2024). The role of information governance in mitigating financial crime risks in stablecoin transactions. *Journal of Engineering Research and Reports*, 26(7), 317-333. <https://doi.org/10.9734/jerr/2024/v26i71212>
- Omolara, P. O., Temitayo, O. A., Azeez, A. A., Fehintola, M. S., Oluwaseun, A. A., & Paschal, M. E. (2024). Encryption techniques for financial data security in FinTech applications. *International Journal of Science and Research Archive*, 12(1), 2942-2949. <https://doi.org/10.30574/ijrsra.2024.12.1.1210>
- Oseremi, O.-O., Yinka, J. O., Nsiong, L. E.-U., & Damilola, O. O. (2024). AI-driven biometrics for secure FinTech: Pioneering safety and trust. *International Journal of Engineering Research Updates*, 6(2), 001-012. <https://doi.org/10.53430/ijeru.2024.6.2.0023>
- Palmer, D. (2008). Extending the process model of collective corruption. *Research in Organizational Behavior*, 28, 107-135.
- Panisi, F. (2017). Blockchain and smart contracts: Fintech innovations to reduce the costs of trust. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3066543>
- Pant, S. K. (2020). Fintech: Emerging trends. *Telecom Business Review*, 13(1), 47.
- Philip Olaseni Shoetan & Babajide Tolulope Familoni. (2024). Transforming fintech fraud detection with advanced artificial intelligence algorithms. *Finance & Accounting Research Journal*, 6(4), 602-625. <https://doi.org/10.51594/farj.v6i4.1036>
- Philippon, T. (2016). *The FinTech opportunity*. National Bureau of Economic Research. No. w22476.
- Pickett, K. S., & Pickett, J. M. (2002). *Financial crime investigation and control*. New York: John Wiley & Sons.
- Puschmann, T. (2017). FinTech. *Business & Information Systems Engineering*, 59, 69-76.
- Puschmann, T., & Alt, R. (2016). Sharing economy. *Business & Information Systems Engineering*, 58, 93-99.
- PwC. (2016). *Blurred lines: How FinTech is shaping financial services*. Retrieved from <https://www.pwc.de>
- PwC. (2021). *Digital banking consumer survey*. Retrieved from <https://www.pwc.com/gx/en.html>
- Ramesh, K., Amudha, R., Prasob, K., & Kanna, K. (2023). Fintech innovations in E-payments: Privacy and security in cybercrime threats. *Multidisciplinary Science Journal*, 5, 2023ss0320. <https://doi.org/10.31893/multiscience.2023ss0320>
- Reurink, A. (2018). Financial fraud: A literature review. *Journal of Economic Surveys*, 32(5), 1292-1325.
- Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change*, 17(2), 164-196. <https://doi.org/10.1108/JAOC-09-2019-0098>
- Rybalchenko, L., Ryzhkov, E., & Ohrimenco, S. (2021). Economic crime and its impact on the security of the state. *Philosophy, Economics and Law Review*, 2, 78-91.
- Saddiq, S. A., & Abu Bakar, A. S. (2019). Impact of economic and financial crimes on economic growth in emerging and developing countries: A systematic review. *Journal of Financial Crime*, 26(3), 910-920. <https://doi.org/10.1108/jfc-10-2018-0112>
- Saluja, S. (2024). Identity theft fraud-major loophole for FinTech industry in India. *Journal of Financial Crime*, 31(1), 146-157. <https://doi.org/10.1108/JFC-08-2022-0211>
- Sampat, B., Mogaji, E., & Nguyen, N. P. (2024). The dark side of FinTech in financial services: A qualitative enquiry into FinTech developers' perspective. *International Journal of Bank Marketing*, 42(1), 38-65. <https://doi.org/10.1108/ijbm-07-2022-0328>
- Sandmo, A. (2005). The theory of tax evasion: A retrospective view. *National Tax Journal*, 58(4), 643-663.
- Sangwan, V., Prakash, P., & Singh, S. (2020). Financial technology: A review of extant literature. *Studies in Economics and Finance*, 37(1), 71-88.
- Sarmah, S. S. (2018). Understanding blockchain technology. *Computer Science and Engineering*, 8(2), 23-29.

- Saxena, A. K., & Vafin, A. (2019). Machine learning and big data analytics for fraud detection systems in the United States fintech industry. *Emerging Trends in Machine Intelligence and Big Data*, 11(12), 1-11.
- Schneider, F., & Windischbauer, U. (2008). Money laundering: Some facts. *European Journal of Law and Economics*, 26, 387-404.
- Schueffel, P. (2016). Taming the beast: A scientific definition of FinTech. *Journal of Innovation Management*, 4(4), 32-54.
- Sironi, P. (2016). *FinTech innovation: From robo-advisors to goal based investing and gamification*. West Sussex, UK: John Wiley & Sons.
- Skan, J., Dickerson, J., & Gagliardi, L. (2016). *FinTech and the evolving landscape: Landing points for the industry*. Dublin: Accenture.
- Slemrod, J. (2007). Cheating ourselves: The economics of tax evasion. *Journal of Economic Perspectives*, 21(1), 25-48. <https://doi.org/10.1257/jep.21.1.25>
- Spreng, R. N., Ebner, N. C., Levin, B. E., & Turner, G. R. (2021). Aging and financial exploitation risk. *Aging and Money: Reducing Risk of Financial Exploitation and Protecting Financial Resources*, 55-73.
- St. Petersburg State University, Belozyorov, S., Sokolovska, O., St. Petersburg State University, Kim, Y. S., & University., G.-W. N. (2020). FinTech as a precondition of transformations in global financial markets. *Foresight and STI Governance*, 14(2), 23-35. <https://doi.org/10.17323/2500-2597.2020.2.23.35>
- Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information & Computer Security*, 26(1), 109-128. <https://doi.org/10.1108/ICS-06-2017-0039>
- Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., . . . Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in Fintech applications. *Sensors*, 21(5), 1594. <https://doi.org/10.3390/s21051594>
- Supervision, B. (2011). Basel committee on banking supervision. *Principles for Sound Liquidity Risk Management and Supervision (September 2008)*.
- Sutton, D. (2022). *Featurespace blocks fraud attacks for financial institutions with AI and NVIDIA GPUs*. Retrieved from <https://blogs.nvidia.com/>
- Tache, C. E. P. (2022). Public international law and fintech challenges. *Perspectives of Law and Public Administration*, 11(2), 218-225.
- Tao, R., Su, C.-W., Naqvi, B., & Rizvi, S. K. A. (2022). Can Fintech development pave the way for a transition towards low-carbon economy: A global perspective. *Technological Forecasting and Social Change*, 174, 121278. <https://doi.org/10.1016/j.techfore.2021.121278>
- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. New York: Penguin.
- The FinTech Revolution. (2015). A wave of startups is changing finance— for the better. *The Economist*, 415(8937), 13.
- Tomasic, R. (2011). The financial crisis and the haphazard pursuit of financial crime. *Journal of Financial Crime*, 18(1), 7-31. <https://doi.org/10.1108/13590791111098771>
- Tran, R. B. L., & Kevin. (2023). *Nelson Mullins - FinTech laws and regulations 2023*. Retrieved from <https://www.nelsonmullins.com/insights/insights/FinTech-laws-and-regulations-2023>
- Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer*, 50(9), 14-17. <https://doi.org/10.1109/mc.2017.3571047>
- Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11, 1-35. <https://doi.org/10.1186/s40163-021-00163-8>
- Uddin, S., Ong, S., & Lu, H. (2022). Machine learning in project analytics: A data-driven framework and case study. *Scientific Reports*, 12(1), 15252. <https://doi.org/10.1038/s41598-022-19728-x>
- Uma, K. E., & Eboh, F. E. (2013). Corruption, economic development and emerging markets: Evidence from Nigeria. *Asian Journal of Management Sciences and Education*, 2(3), 56-67.
- Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive*, 11(1), 1810-1817. <https://doi.org/10.30574/ijrsra.2024.11.1.0284>

- Uña, G., Verma, A., Bazarbash, M., & Griffin, M. N. N. (2023). *FinTech payments in public financial management: benefits and risks*. International Monetary Fund. <https://doi.org/10.5089/9798400232213.001>.
- Ungureanu, M.-A., & Filip, L.-M. (2023). The rise of FinTech and the need for robust cybersecurity measures. *EIRP Proceedings*, 18(1), 549-559.
- Ünvan, Y. A. (2020). Financial crime: A review of literature. *Contemporary Issues in Audit Management and Forensic Accounting*, 102, 265-272. <https://doi.org/10.1108/s1569-375920200000102019>
- Utkina, M. (2023). Digital identification and financial monitoring: New technologies in the fight against crime. *Scientific Journal of Polonia University*, 58(3), 303-308. <https://doi.org/10.23856/5842>
- Verhoef, P. C., Kannan, P. K., & Inman, J. J. (2015). From multi-channel retailing to omni-channel retailing: Introduction to the special issue on multi-channel retailing. *Journal of Retailing*, 91(2), 174-181. <https://doi.org/10.1016/j.jretai.2015.02.005>
- Villányi, B. (2021). Money laundering: History, regulations, and techniques. In *Oxford Research Encyclopedia of Criminology and Criminal Justice*.
- Vuković, D. B., Hassan, M. K., Kwakye, B., Febtinugraini, A., & Shakib, M. (2024). Does fintech matter for financial inclusion and financial stability in BRICS markets? *Emerging Markets Review*, 61, 101164. <https://doi.org/10.1016/j.ememar.2024.101164>
- Wang, J. S. (2021). Exploring biometric identification in FinTech applications based on the modified TAM. *Financial Innovation*, 7(1), 42. <https://doi.org/10.1186/s40854-021-00260-2>
- Wang, X., Xue, H., Liu, X., & Pei, Q. (2019). A privacy-preserving edge computation-based face verification system for user authentication. *IEEE Access*, 7, 14186-14197. <https://doi.org/10.1109/access.2019.2894535>
- World Bank. (2022). *Financial inclusion overview*. Retrieved from <https://www.worldbank.org/en/home>
- World Economic Forum. (2022). *Global risks report 2022*. Retrieved from <https://www.weforum.org/>
- Yahaya, M. H., & Ahmad, K. (2018). *Financial inclusion through efficient zakat distribution for poverty alleviation in Malaysia: Using FinTech & mobile banking*. Paper presented at the Proceeding of the 5th International Conference on Management and Muamalah. pp. 15-31.
- Yenkey, C. B. (2018). Fraud and market participation: Social relations as a moderator of organizational misconduct. *Administrative Science Quarterly*, 63(1), 43-84. <https://doi.org/10.1177/0001839217694359>
- Yerram, S. R., Goda, D. R., Mahadasa, R., Mallipeddi, S. R., Varghese, A., Ande, J., . . . Dekkati, S. (2021). The role of blockchain technology in enhancing financial security amidst digital transformation. *Asian Business Review*, 11(3), 125-134. <https://doi.org/10.18034/abr.v11i3.694>
- Zakaria, P. (2023). Financial inclusion to digital finance risks: A commentary on financial crimes, money laundering, and fraud. In *Financial Technologies and DeFi: A Revisit to the Digital Finance Revolution*. In (pp. 123-130). Cham: Springer International Publishing.
- Zeidy, I. A. (2022). *The role of financial technology (FinTech) in changing financial industry and increasing efficiency in the economy*. COMESA Monetary Institute. Retrieved from <https://www.comesa.int/wp-content/uploads/2022/05/The-Role-of-Financial-Technology.pdf>
- Zhu, Y., Li, X., Wang, J., & Li, J. (2020). Cloud-assisted secure biometric identification with sub-linear search efficiency. *Soft Computing*, 24(8), 5885-5896. <https://doi.org/10.1007/s00500-019-04401-9>

*Views and opinions expressed in this article are the views and opinions of the author(s), Financial Risk and Management Reviews shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.*