# Cybercrime and Cyber Security in Fintech


**Anastasija Despotović, Ana Parmaković, and Marija Miljković**

**Abstract** This paper describes cybercrime in the field of financial technologies. There have been significant changes in payment systems caused by the development of Fintech and the increasing use of various digital and mobile technologies. Methods of protection against cybercrime are being developed in parallel with the development of new technologies, but cybercrime is also progressing at the same pace. The perpetrators are constantly finding new ways to abuse financial systems. Users of financial technologies must be aware of the potential risks of using financial technologies, only in that way will they be able to recognize and prevent potential threats. The increasing use of cryptocurrencies and the lack of legal regulations have led them to become a valuable target for criminals, and the number of crimes connected to cryptocurrencies is constantly growing. This paper aims to acquaint readers with the dangers of cybercrime and methods of protection against them. The first chapter of the paper is an introduction in which the concepts of cybercrime and cyber security are defined. The second chapter identifies and describes the threats and dangers of cybercrime in financial technologies. Chapter 2 deals with the analysis of current threats to financial systems as well as modern ways of protecting financial systems from cybercrime. How cyber-attacks manifest themselves and how attacks can be prevented are defined and explained. Different types of cyber-attacks are described in detail. The analysis led us to the conclusion that it is best to prevent cyber-attacks and that employee training is a very important factor in protecting the system so that they know how to prevent potential attacks and accidental security breaches. Chapter 3 analyzes the literature dealing with cybercrime and cybersecurity in the field of financial technologies. The literature states that banks were the first to introduce technological innovations into their operations, which led to the

A. Despotović · A. Parmaković (✉)
Faculty of Organizational Sciences, University of Belgrade, Belgrade, Serbia
e-mail: ana.parmakovic@stadaitsolutions.com

M. Miljković
Directorate for Telecommunications and Informatics J-6, Center for Command and Information Systems and Information Support, Belgrade, Serbia
e-mail: marija.miljkovic@vs.rs



S. Benković et al. (eds.), *Digital Transformation of the Financial Industry*,
Contributions to Finance and Accounting,
https://doi.org/10.1007/978-3-031-23269-5_15

revolution of technological progress in Fintech. Not only do banks participate in modern financial business, but a significant part of the business also consists of companies that specialize in the development and implementation of financial technologies. The fourth chapter deals with identified problems and potential solutions. Chapter 4 identifies problems and potential solutions in the field of financial technologies. The vulnerability of financial systems, how cyber-attacks take place, and their adaptation to modern business are analyzed. Based on the analysis, potential solutions to the identified problems are given and specific examples are given. The analysis led us to the conclusion that we must consider cyber risks in detail and give an adequate counter-response to each of their elements. The fifth chapter deals with cryptocurrencies. Blockchain technologies, their level of security, ways of endangering as well as their impact on financial operations are analyzed. The problem of lack of legal regulations in the field of cryptocurrencies is explained, as well as their impact on the growth of cybercrime in the field of financial technologies. The sixth chapter concludes the paper. The seventh chapter presents a list of references used in the paper. The main contribution of the paper is the systematic analysis of cyber threats and cybersecurity issues in the context of Fintech, resulting in a list of recommendations for various groups of stakeholders (banks, fintech companies, and end users).

**Keywords** Cybercrime · Cybersecurity · Financial technologies · Cryptocurrencies · Financial system

## 1 Introduction

Innovations in the field of technology always carry with them a certain type of risk, so it is necessary to foresee the risk factors before implementation and prevent them, prevent their manifestation in the process itself, and also prevent the appearance of new threats. The mentioned measures should be applied by every technologically developed company, especially companies that rely on the electronic business for a large part of their work. The aforementioned challenges are imposed by criminal entities in cyberspace who, we can safely say, adequately use the current technological development themselves. We see, therefore, that it is necessary to ensure the protection of vulnerable parts of the infrastructure and advanced defense of systems, servers, networks, computers, mobile devices, etc., which establishes a certain level of security in cyberspace. In which "cyberspace" represents the connection of computer networks, as it were, and the techniques of their protection "cyber security."

Cyber security (cyber security, cyber protection, digital security) is, in the simplest terms, the practical protection of devices, resources, and information (accounts, personal data, files, and of course money). To properly protect something, the most important thing is to ensure: confidentiality, that is, the independent possibility of controlling the authorization to access one's accounts, so that

information does not leak; integrity of the data in our possession, i.e., knowledge that no one could change them without our permission; Access or the ability to access resources in our possession when we want it, that is, that access is not denied to us caused by cyber-attacks, such as DDoS or Ransomware. Opposing and avoiding malicious actions and their consequences requires analysis of the forms in which threats are manifested, and then synthesis of knowledge into responses to them. This is a particularly demanding job when we cannot determine the exact location of the malicious entities, and they are in most cases potentially close to us and possess the necessary means and information to carry out the attack. Employee education is crucial, to reduce the percentage of work errors, and also to train them for correct and ethical work.

There is no modus operandi, that is, a universal way of behavior of criminals in cyberspace, and thus not all directions of the spread of cybercrime can be described. However, as every criminal behavior needs to be defined by law, cybercrime (in legal regulations and high-tech crime) is most often described as any criminal offense in which the object, goal, or means of its execution is a computer, computer systems, networks, computer data, and/or their resources in material or electronic form. The convention on high-tech crime distinguishes four types of criminal acts, namely: acts against confidentiality, acts related to computers, acts related to the content, and acts related to copyright infringement.

As we emphasized at the beginning, technological development also influenced the more professional activities of criminals, and this trend did not bypass financial technologies either. Fintech as a new wave of financial business improvement provides numerous benefits, so user satisfaction is on the rise, but it also represents a very tempting area for criminal activities, primarily due to the constant flow of money, and material gain is one of the main motives for any criminal behavior. However, intangible consequences can also have a permanent impact on the business, in terms of loss of trustees, bad publicity, loss of protected information, etc. We realized that it is of great importance to protecting given values within financial institutions, and it is precisely this thought that guides us throughout our work.

## 2 Identification, Description of Threats and Dangers of Cybercrime in Fintech

The use value of money makes it one of the most tempting targets for cyber-attacks. Financial institutions that store a large amount of data about bank accounts and identities of users of financial services are frequent targets of attacks by cybercriminals.

The financial services sector increasingly relies on modern information and communication technologies to provide products and services to clients. The use of new technologies to a greater extent requires changes in procedures and

regulations in the banking sector, including constantly changing rules on privacy and data protection, as well as cyber security requirements.

In a world of rapid technological changes, judicial authorities are introducing more rigorous data protection laws, individual responsibility is growing, and penalties for fraud are increasing. There are also many court cases related to intrusions into financial systems.

After detecting a large number of work interruptions in banks and companies, drafts are designed, and more adequate measures are taken to protect the system infrastructure and client privacy in the digital environment. There is an increased focus on business continuity, the resilience of the infrastructure is strengthened, and more modern methods of protection are applied.

Financial enterprises are evaluating the potential attack vectors they encounter daily. Special attention is also paid to the training of internal staff on the classic profiles of cybercriminals to gain a better insight into the threats they face knowingly or unknowingly.

Cyber-attacks in the financial sector are more destructive and pronounced compared to other sectors. Security threats can have a significant impact on the entire economy of a country or region. Money is generally the main motive for carrying out the attack. In addition, employees may be persuaded to provide vulnerable information to potential attackers in exchange for their gain.

## *2.1 The Most Significant Attacks in the Financial Sectors*

Some of the most common cyber threats in the financial sector are Phishing, Ransomware, DDoS, Supply Chain, Bank Drops, and ATM Jackpotting.

### 2.1.1 Phishing

Phishing is a version of social engineering that misuses user data that including login credentials and credit card numbers. The attacker uses the spoofing technique to disguise himself as a trusted entity through a legitimate means of communication to deceive the victim. A potential victim receives a malicious email that may initiate the installation of malicious software on the targeted computer system or load a fraudulent web page that collects login credentials.

An attack can have devastating consequences, including unauthorized purchases and misuse of assets and identities. Installing malicious software on a large number of computers can initiate the creation of a foothold in corporate networks. In such a scenario, employees are compromised. They distribute malware within a closed environment and can be used as assets in large-scale attacks against appropriate targets. An organization exposed to such an attack suffers significant financial losses, reputation, and consumer trust.

Preventive computer protection against phishing attacks is the use of antivirus software. Automatic updating of the antivirus solution is essential, providing optimal protection and dealing with current security threats in real-time. Multi-factor authentication (MFA) is an important component of good identity and access management (IAM). MFA offers additional security by requiring additional verification factors in addition to the username and password requirements, thus allowing access to online resources and reducing the possibility of a successful cyber-attack. Note that having two different passwords is not considered two-factor authentication (Ramzan 2010).

Data backups at other locations prevent data loss in the event of an attack or equipment failure and are an important part of a successful disaster recovery plan.

### 2.1.2 Ransomware

Ransomware hacking groups often target financial industries for valuable customer information. The primary targets of the attacks were personal computers, but the attackers focused on corporations that store large amounts of confidential data about users, and often pay to unlock it.

The two most prevalent types of ransomwares are encryptors and screen lockers. Encryptors encrypt data on a system that is impossible to access without a decryption key. While the screen lock blocks access to the system noting that the entire system is encrypted.

Ransomware is a type of malware that encrypts data and blocks access to a computer system and data until the victim pays appropriate financial compensation. Infection usually starts with a malicious email. If a user opens an email or clicks on a malicious URL, the malicious software is installed and begins to encrypt essential files on the victim's computer. After the data encryption process, a notification is displayed on the compromised device. Encryption ransomware works by obfuscating the contents of user files using strong algorithms (Mohurle and Patil 2017). The notices contain a payment procedure to the attackers for the process of decrypting the compromised data. The request is time-limited and the appropriate financial compensation must be paid. To pay the ransom, the attackers use different methods of extortion to increase the pressure on the victims. The danger of leaking this data on the dark web can cause great damage to the reputation of companies that offer financial services and comply with ransom demands. After the payment has been made by the victim, the data is decrypted. There is a high probability that due to the paid fees, the victim will never receive the keys to decrypt the data. Experts think that no ransom should be paid, but many organizations have no choice. Payment is mostly made in cryptocurrencies.

Preventing ransomware attacks involves making backups and applying for adequate protection with security tools. Email protection tools are the basic line of defense, while endpoint data on workstations is a supplementary defense. Intrusion detection systems (IDS) are used to detect attacks. User training is important, but it is only one of several layers of "Defense in Depth" defenses.

### 2.1.3 DDoS Attacks

Despite the emergence of the cryptocurrency industry like Bitcoin and the constant growth trend of attacks on them, the financial field still suffers from a large number of Distributed Denial-of-Service (DDoS) attacks. The majority of DDoS attacks against targets in this sector hit the application and network layers of the TCP/IP reference model. DDoS attacks are a widespread potential threat to financial services because their attack domain is heterogeneous, including IT infrastructure, online trading platforms, user accounts, transaction websites, etc. This type of attack is implemented using so-called Bots and BotNets.

A botnet is a network of infected computers on the Internet that can be remotely controlled, used to send SPAM email, or organize DDoS attacks. A BotNet is also called a Zombie Network, where an individual computer is called a Bot or Zombie. A large number of computers around the world are believed to be part of one of the BotNet networks. These are mostly home PCs, without adequate Firewall and AntiVirus protection. They are also the starting point for launching DDoS attacks on financial companies.

Cybercriminals use various tactics to compromise and steal financial and private data. The Cybercrime as a Service (CCaaS) business model is used to implement DDoS attacks. It is designed so that an experienced cybercriminal builds advanced tools, software, and services to rent and sell to less experienced cybercriminals. As a result, attackers with limited expertise and a lower level of knowledge carry out attacks without much difficulty.

During the execution of the attack, the victim's server or network is flooded with fraudulent requests. Due to the high concentration of illegitimate requests from thousands of computers, attackers try to overload the computer network, servers, or some part of the IT infrastructure, thus preventing the normal functioning of systems and services. A successfully executed attack disables access to copper websites or Internet services. Customers become prevented from accessing and using their financial services and data. The consequences are loss of income, work of reputation, and violation of clients' trust in the functioning of the institution.

Large companies tend to protect themselves from security challenges, risks, and threats caused by the occurrence of DDoS attacks. Organizations implement effective security protections against DDoS attacks. The basic step in the protection process is to increase the bandwidth of the infrastructure. This method should be combined with other adequate means of protection. The use of hybrid cloud services increases security and provides optimal security due to the provision of unlimited bandwidth. It is crucial to create a DDoS Response Plan where every step is described in the event of an established attack, which provides additional security. The plan includes defined procedures, checklists in the system, and a qualified response team. A predefined plan provides a quick and efficient response. Time is a very critical factor in these cases. Every hour of downtime causes companies to lose serious amounts of money, so it is necessary to respond quickly to the incident.

### 2.1.4 Attacks on the Supply Chain

A supply chain attack is a type of cyber-attack that targets organizations that have potentially weak links in the supply chain. The supply chain primarily refers to the delivery of goods from the supplier through the manufacturer to the end user, networked individuals, organizations, technologies, services, resources, and activities that participate in the cycle from creation to sale of products. The weakest link and target of attack in this process are third-party suppliers, such as the financial or government sectors, that are closely related to the actual target.

An attack infiltrates a system to cause loss to the organization. Malicious programs are embedded in software or hardware that is trusted and already widely used, so the attacks themselves are very difficult to detect.

Proper third-party risk assessment is a priority and imperative to prevent supply chain attacks. By reducing the number of employees in the organization who are authorized to install software or introduce third-party hardware, the size of the attack can be reduced. Of particular importance is limiting access to confidential data and developing a stronger cyber security strategy.

### 2.1.5 Bank Drops

To hide the location and storage of stolen money, cybercriminals often store the stolen funds in fake bank accounts that they open with the stolen credentials of existing bank customers. The victim's complete user data is called "full" by cybercriminals. "Fullz" data can be purchased on the dark web and the price varies depending on the number of records. This data includes information about the potential victim, such as first name, last name, address, DOB (Date of birth), credit score, social security information, account numbers, driver's license number, etc. The patterns by which these attacks are carried out tend to shift to the digital wallet as more and more attackers choose cryptocurrencies that provide them with anonymity.

In response to this threat, financial institutions are required to perform special security checks on the credentials that have privileged users to open new accounts.

### 2.1.6 ATM "Jackpotting"

ATM Jackpotting is an attack on the physical and software vulnerabilities of Automated Teller Machines (ATMs) that ultimately have the ATMs disbursing cash. In this type of attack, cybercriminals suddenly get huge sums of money from ATMs (Kasanda and Phiri 2018). The money that the attacker steals is not tied to any bank account but is a cash payment of reserves from the ATM itself. The means used for this type of attack is a laptop or device that physically connects to the ATM and contains malicious software in the operating system that accesses and takes control

of the ATM's main controls. The most common targets are stand-alone ATMs, which do not have strict supervision, adequate security, and updated software.

To prevent these increasingly sophisticated attacks, it is necessary to regularly update the software for better defense. Define a white list and lock the system to prevent the use of unauthorized programs and external media to prevent the entry of malicious software into the operating system of the ATM. Implement default passwords and update them. Then enable physical security and surveillance of ATMs to prevent unauthorized actions.

## 3 Literature Analysis

### *3.1 Fintech*

There are many definitions of financial technologies, one of the most famous is: "Fintech is a new financial industry that applies various technologies to improve financial activities" (Schueffel 2016). The financial technology industry includes several innovative technologies based on powerful and complex analytical tools, advanced algorithms, software applications, big data as well as many other different functionalities (Spulbar et al. 2020). Fintech enables financial transactions to be carried out via digital devices such as mobile phones, tablets, computers. The application of financial technologies implies working on innovations and improving the quality of financial services by adapting technical solutions to different situations (Leong and Sung 2018). The goal of Fintech and the companies that deal with them is to help traditional companies implement modern technical solutions to improve their business. The use of different technologies and services is used to achieve the greatest possible efficiency so that clients are as satisfied as possible (Spulbar et al. 2020).

The connection between technology and the financial sector has a long history, from the introduction of the telegraph in the early 1800s to the first ATM installed by Barclays Bank in 1967, today we are in the Internet era, where technology is essential for both banks and customers (Arner et al. 2015). Banks are the most important part of the financial systems and they were the first to apply technological innovations to their financial systems. According to Nikkel, the idea of ATMs was a revolutionary idea at the time, as was the development of telephony systems on personal computers with modems to access banking applications. Since the expansion of the Internet in the 1990s, banks have developed online banking for consumers, while MasterCard has provided the latest technologies for online shopping (Nikkel 2020).

During the last decade, numerous companies dealing with financial technologies and cooperating with financial institutions have been formed. Fintech companies are taking advantage of financial technology to meet increasingly complex customer requirements, address compliance barriers, achieve high growth, and implement innovative business models (Pollari 2016). Financial technology advances facilitate

financial inclusion, greater use of financial services enabling applications, reliability, and fairness of financial transactions, new market opportunities for smaller companies, and competitive advantage for entrepreneurial companies (Medeiros and Chau 2016). One of the main advantages of Fintech companies is that they reduce public distrust of the traditional financial industry because financial transactions are fast, secure, and transparent to the customer (Rooney et al. 2017). Banks cooperate with Fintech companies precisely for the above reasons. One of the problems that occur in the cooperation of banks with Fintech companies is the alignment of companies with the rigid structure of banks, as well as compliance with all procedures and regulations that banks must follow (Milne 2016). The biggest problem faced by banks that cooperate with Fintech companies is in the formation of common standards because they usually do business in different ways. Fintech innovations are characterized by many advantages, the most significant of which is the increase in customer satisfaction in the evolution of the global financial system. Significant changes in the financial sector have resulted in vulnerabilities that allow cyber-attacks, especially bank fraud. Potential risks related to the Fintech industry must be reduced by implementing the following activities: consumer and investor protection, clarity, and consistency of regulatory and legal frameworks (Spulbar et al. 2020).

## *3.2 Cybercrime*

Cybercrime refers to any illegal activity that is carried out using a computer or the Internet (Avast 2022). Cybercrime is on the rise, and the emergence of new technologies such as AI, big data, and the cloud provides criminals with opportunities for new abuses of the system. Fintech start-ups, banks, and other financial institutions are at risk of various attacks, and the application of new technologies makes them targets for cybercriminals. Cybercrime includes certain categories, such as electronic fraud, cyber espionage, malware attacks, identity theft, cyberstalking, spam, copyright infringement, cyber terrorism, and computer viruses (Spulbar et al. 2020). Internet banking is a relatively new component of the banking system, very attractive, but also very vulnerable to cyber-attacks. Cybercrime activities are very difficult for law enforcement. Cybercrime brings great material damage, but non-material damage is also very significant (Antonescu and Birau 2014). Highlighting the non-financial consequences of cybercrime, such as the following: loss or violation of consumer trust, disparagement campaign based on negative publicity (bad image, public defamation, damage to reputation and prejudice), discontinuity and interruptions in business, reductions in productivity, compromising confidential customer data, unauthorized and prohibited access to various product innovations, misuse of intellectual property, as well as many other categories.

The main difference between Fintech start-ups and banks is that banks and other financial institutions invest large amounts of resources in the fight against cybercrime, data theft, and fraud defense and have established regulations to prevent cybercrime that poses a threat to the financial stability of the institution (Adeyoju

2019). Cybercrimes represent a financial loss for financial institutions and a reputational risk for them. Cyber breaches lead to loss of customers, reputation, revenue, brand, capital value, and higher operational costs for Fintech firms (Kopp et al. 2017).

Many tools that are legitimate help criminals in their abuses, such as cryptocurrencies and VPNs. VPN providers resist providing information to the police because they base their business on security and anonymity and refuse to admit that they are helping cybercriminals.

During the Covid-19 pandemic, users of financial services massively switched to conducting financial transactions via mobile devices, as a result of which there was an increase in the number of mobile banking trojans. A banking trojan/banking malware is a malicious computer program that attempts to gain access to confidential information stored or processed through online banking systems. A Trojan horse is any type of malicious program disguised as legitimate (Kopp et al. 2017). Malicious virtual applications represent one of the most prolific forms of cybercrime.

The shadow economy helps criminals achieve their abuses. The lack of regulation in many countries allows various services to conduct their business, such as cryptocurrencies and bulletproof hosters. The European Union has introduced the "5th Anti-Money Laundering directive" which regulates cryptocurrency transactions within the EU. There is no similar regulation at the global level (IOCTA 2021). Action to effectively fight cybercrime is based mainly on a clear and predictable legal framework. Enforcing rigorous cybersecurity standards is essential to reducing the effects of cybercrime (Spulbar et al. 2020).

### *3.3 Cyber Security*

FinTech solutions rely heavily on technologies that are prone to hacking and data that is susceptible to abuse and manipulation, their combination can often lead to disastrous consequences (Adeyoju 2019). Cyber security can be defined as the security of information and the protection of electronic systems, networks, devices, programs, or data from theft or damage (Schatz et al. 2017). For the above reason, cyber security is one of the most important factors in financial technologies. As people and businesses around the world become increasingly dependent on modern technology, vulnerabilities to cyber-attacks such as corporate security breaches, phishing, blackmail, and social media scams are increasing. (Stevens 2018). Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks, it includes the security of information technologies as well as the security of electronic information (Kaspersky 2022). Devices are increasingly connected and it poses an additional threat to cyber security and makes companies vulnerable to attacks. Companies that implement financial technologies are vulnerable to various attacks because they possess the confidential data of their customers. According to Najaf, the most

common cyber security threats are Malware attacks, Data leakages, and Data integrity risks (Najaf et al. 2021).

The vulnerability of companies and the frequency of attacks have led to great efforts by experts and researchers to apply smart technologies such as artificial intelligence and other analysis tools to be able to counter cyber-attacks before they happen (Kang and Kang 2016). Smart programs and competent programmers are used to detect and classify malicious programs, stand up and address them, address their implications, and set protocols to prove the identity of users in the program (Al-Maksousy 2018). According to Davis, two types of risks are considered the strongest, the first are users of the system and others on the server side, where the data is stored (Davis 2017). Securing cyberspace is particularly difficult due to many factors: the ability of evil actors to operate from anywhere in the world, the existence of links between cyberspace and physical systems, and finally, the difficulty of reducing vulnerabilities and consequences in complex information networks (Al Duhaidahawi et al. 2020). Despite attempts to secure information infrastructure, employees in organizations still represent the biggest threat to cyber security, so it is necessary to focus on the behavior of employees in the organization. There is no one-size-fits-all solution to preventing cybercrime. Companies must regularly educate their employees about current threats so that there are no work errors that lead to phishing attacks or the installation of malware. A risk management plan is an important part of system protection. Threats must be assessed and an appropriate protection plan made.

To stay protected and safe from cyber-attacks, Fintech companies and banks must make continuous employee education a priority. They must train their staff and teams on data protection and disaster management, build and maintain a cyber security infrastructure designed to detect, withstand and repel cyber threats and report cyber-attacks promptly, as required by law (Adeyoju 2019).

## *3.4 Analysis of Research Results*

There is no universal definition for Fintech, each author who deals with the mentioned field offers his own, which he believes should be generally accepted. The authors believe that the development of technology directly affects the financial systems and that they form a whole that cannot do without each other. Banks have always been the most important financial institutions and have always accepted the use of new technologies, in the past, it was ATMs, and in modern business, we can cite e-banking platforms as an example. Fintech enables greater involvement of the people, as it allows the people to do their financial affairs from home through various devices such as mobile phones, computers, or tablets. Fintech introduces significant changes in traditional business, resulting in new system vulnerabilities. Potential risks must be minimized. The authors agree that cybercrime is on the rise. New ways of conducting illegal activities and abusing fintech systems and technologies are constantly being found. The lack of legal regulations also affects the occurrence of

cybercrime, because there are no legal regulations at the global level, in some countries e-business and fintech are just at their beginning, and therefore legal regulations. The consequences of cybercrime can be tangible and intangible. Companies that have suffered a security breach often suffer damage to their reputation, which is sometimes more difficult to recover than material damage.

The authors define cyber security as the protection of information and electronic systems from theft or damage. As fintech solutions rely heavily on technologies that are prone to hacking and various attacks, cyber security is one of its most important factors. Cyber security experts are putting a lot of effort into developing tools to prevent cyber-attacks and crime. Smart tools are used to detect and prevent unwanted system intrusions.

## 4 Identified Problems and Potential Solutions in Fintech

Before identifying the problem and stating possible solutions, it should be said that it is most profitable to assume and prevent any potential security threat, especially in the field of financial technologies. It is necessary to make an adequate assessment of potential risks and an empirical assessment of those risks that we may have exposed ourselves to in the past, without reacting correctly at that time. Thus, based on previous knowledge, we will be able to analyze their ways of acting and respond to them concretely.

In the past, financial fraud was based on transactions, from which entities defended themselves with regular and direct controls. Today, thanks to applications that exploit user data, identity-based fraud is more common. Also, their work is not monitored by appropriate supervisory bodies. With the development of financial technologies, the number of threatening entities also grows, because it is not entirely possible to provide the highest quality services in this area, without putting user security into question. Adding new user benefits and other functionalities makes it harder to protect trusted user data and increases system vulnerability. Now, more work must be done to prevent third-party intrusions, so that they do not provide themselves with access to protected data.

Confidentiality, integrity, availability, authentication, and non-repudiation are commonly cited as data protection objectives. Confidentiality presupposes the aforementioned prevention to prevent unauthorized data access, and it should ensure the privacy of the exchanged data. Integrity prevents unauthorized information from being changed so that the exchanged data reaches the final destination unchanged. Availability refers to the prevention of sabotage of access to information or resources of importance. Authentication prevents impersonation and non-repudiation is achieved precisely by preventing the masking of the entity from which the malicious activity originates; both objectives can be ensured by applying a digital signature.

Cyber-attacks in Fintech are a common occurrence. This is best seen through the establishment of cooperation between traditional financial companies (banks) and Fintech firms as modern financial providers, where the leakage or loss of data caused

by cyber-attacks can have a fatal outcome. We are talking about user credentials and payment card data. In recent research, it is stated that this type of theft of data in the possession of banks is on the rise after the establishment of their cooperation with fintech companies because they are not able to adequately protect them (Ozili 2018).

Also, customized malicious attacks on SWIFT (Society for World Interbank Financial Telecommunication) are becoming more common. SWIFT is used for the international exchange of data between the banks of the world, through digitized communication. The system itself provides a degree of protection depending on the importance of the data exchanged, but recent research shows that even its systems are vulnerable to increasingly sophisticated attacks. The most exposed to them are banks that have established a regulator within Fintech, which allows its start-ups to conduct controlled experiments on their environment, thus creating an unstable environment suitable for hacker work.

These companies base their business on cloud computing, which does not have prescribed measures for saving data, which is why there is a potential loss of data. Cloud computing enables online payments, the use of digital wallets, and all in all, faster payment transactions. Protecting such business dynamics is a real challenge, requiring compliance with a whole range of security regulations and the use of adequate encryption techniques to protect sensitive information.

Concrete steps must be taken in the field of Fintech to improve the security situation and the protection of users. Potential solutions should integrate the importance of business priorities, but also their quality protection. In general, protection measures can be described as a continuous process that practically never ends and starts with prevention measures such as firewall, configuration, change of default credentials by the administrator, and the like. Then comes detection, i.e., detection of already damaged or attempted damage to the installed protection. Detection is achieved through continuous monitoring of the work of both external and internal factors. Also, for this purpose, intrusion detection systems are being developed, which, based on a memorized database, notice unusual activities and notify administrators about them. After which the reaction follows, i.e., taking steps to recover stolen data or restore the entire system if changes occurred during those detected unusual activities. It eliminates the consequences and it is desirable to return the system to its original, if not improved state.

The most commonly used answer to protect sensitive data is access control and for that purpose the use of the aforementioned cryptography, which enables communication even over an insecure communication channel by encrypting data so that an attacker cannot break the code. Risk reduction and prevention can also be established by physical methods, i.e., physical application of changes directly to the infrastructure, thus preventing further network damage. Then, by introducing access control lists that are used as a mechanism to protect the data warehouse and secure the cloud environment. They are applicable when exchanging different contents or when it is necessary to delete certain stored data. Based on all of the above, we can conclude that we must analyze cyber risks and provide an adequate counter-response to each of their elements.

### *4.1 Guidelines for Future Research in the Field of Financial Technologies*

Fintech companies must coordinate their work with the banks and companies they cooperate with, to protect their business through joint efforts, especially from cyber-attacks. Also, compliance with legal frameworks and internal regulations is mandatory, especially the application of the Law on Consumer Protection and Electronic Commerce. It is also important to establish an economic balance between the promotion of innovations in financial technologies and the regulation of the traditional way of working in financial companies.

Future research related to financial operations and fintech should:

- Instruct fintech companies not to keep problems related to cyber security in business a secret, where they are difficult to access but to create an action plan with the help of the acquired knowledge in the event of a recurrence of cyber-attacks of the same or similar type.
- Study the impact of cyber security issues on fintech, as well as their impact on partnerships with banks. What are the assessments of traditional banks' trust in fintech, after taking measures to prevent cyber-attacks or after the consequences of a certain malicious action, if it happened.
- Expand the field of research using systematic econometric models, such as the ordinary least squares model or the probit model.

## 5 Cryptocurrencies

Blockchain is currently one of the most popular and significant technologies of today. Most people have heard of the term, but the concept behind it is still unknown and not clear enough. This technology is the basic model on which the operation of cryptocurrencies is based. Blockchain consists of a chain of records called blocks in which information is arranged in a certain order. Each block consists of a defined number of transactions, and each transaction is stored as the output of a hash function. A hash is an authentic address that is rewritten to each block in the process of its creation and any change in the block results in a change in its hash value.

Every work and decision is based on the agreement of all nodes of the network participating in the work of digital currencies. The processed data is encrypted with the help of cryptographic algorithms and functions to ensure user privacy and data integrity. Strong and complex encryption algorithms provide them with optimal protection.

The entire system of blocks and information is managed in a decentralized way, there is no central authority that performs the administration. In this way, there is no type of control by the government or any central entity, unlike other payment

systems. As a result, we have that the third party, i.e., banks or government have no role in this concept (Hughes 2017).

Durability, robustness, reliability, and transparency are some of the characteristics of Blockchain. By design, Blockchain is designed to work as a medium of exchange online for purchasing goods and services and making payments.

One of the originally used cryptocurrencies in the world is the famous Bitcoin digital wallet founded in 2009. Bitcoin works on Blockchain technology and is used as a digital form of cash for payment. Its use is based on the trade of everyday things, there is also the possibility of larger purchases such as cars and real estate.

Physical money is transferred and exchanged in the real world, while cryptocurrency payments exist as digital entries in an online database that have a description and specific characteristics of the completed transaction. Crypto transactions are always successful, there are no delays and procedural costs.

Cryptocurrencies are forms of currency that exist in digital form and are stored in digital wallets. It is possible to buy them with the help of Digital wallets or trading platforms. They can be digitally transferred during trades in cyberspace, while blockchain technology stores and records the transaction and the new owner. The convenience of cryptocurrencies is that there is a record of all performed activities, i.e., the transfer of digital currency assets, and they are kept in a public ledger (digital ledger). After saving the data in the form of a digital ledger, the data is replicated on each node across the entire blockchain network, which makes it safer and impossible to change, hack, or defraud the system. The advanced coding method is used to store and transfer cryptocurrency data between wallets and public ledgers. Thanks to Blockchain technology, cryptocurrencies are immune to counterfeiting and reliable because every transaction is recorded. Verification is achieved by encryption by each node, i.e., member to complete the transaction. Cryptocurrencies got their name based on the application of cryptographic algorithms for the realization of transactions.

Digital transactions are encrypted, creating an undeniable, time-registered, and secure record of every payment, purposefully protecting against third parties with ulterior motives. Block sets record information about transactions, for example: who are the actors of the transaction, the direction of the transaction, and the amount of trade. This system is a peer-to-peer system that allows anyone regardless of location to send and receive payments (Hughes 2017).

Blockchain technology has the potential to transform the entire financial sector because it brings a significant number of benefits such as lower costs in the business, quick execution of transactions, the ability to review executed operations, and other advantages. Cryptocurrencies have revolutionized the world of finance and banking.

However, banks are afraid of the potential risks of this technology because there are almost no regulations regarding digital trade. One of the reasons for concern is the security and stability of cryptocurrency, which is why legislative entities are wary of any business in this area. The decentralized nature of the currency undermines the authority of central banks because there is a belief that they will be almost unnecessary in future operations.

There is also huge potential for economic growth, although there is a chance for criminal activity. Compliance guidelines should be defined to help banks bring innovation and efficiency to crypto-business.

Financial institutions should consider the crypto-competitor as a possible partner and become part of the crypto-industry. Banks could add the necessary security to this unregulated environment.

Banks must find a way to embrace this technology. By recognizing the potential benefits, they could improve financial services and alleviate current concerns.

Bitcoin has shown that the underlying security of its proof-of-work system is solid, however, there are limitations to this system. Limited scalability, high energy consumption, and unstable concentration of mining funds. There have been many scams from centralized brokers and promoters of cryptocurrency IPOs. Manipulation is very widespread in cryptocurrency exchanges. Money laundering and other criminal activities are serious problems in this area. Cryptocurrency is becoming the preferred payment method for all types of scams. The whole concept of digital currencies is widely accepted, but there is also an increasing rate of exploitation by hacker attacks and criminals who finance their illegal operations on the dark web.

## 6 Conclusion

Money in any form attracts unwanted attention from criminals. As a consequence of technological development, cash is in less and less use, thus the use of electronic money has grown. Countries like Sweden want to phase out physical money completely in the next 5 years and completely switch to the use of digital payments. The main advantage of digital payments and money transfers is that it is possible to easily follow the trail of money, which is not easy when using cash. Monitoring digital transactions significantly reduce the possibility of simple "money laundering," as well as the use of money in various illegal activities. As a result of these changes, criminals had to come up with alternative ways to continue their illegal activities.

Financial institutions, as well as financial technology companies, must prioritize the protection of their systems as they are prime targets due to the growth in the use of digital payments. Zero-day threats appear every day that cannot be prevented, therefore it is important to actively monitor all vulnerabilities in systems and remediate them in time. Unfortunately, no software can prevent all dangers and threats from unwanted intrusion into the system. The key to system protection is regular system maintenance and various employee training. Many organizations often neglect the training of employees, who can prevent a significant part of the attacks that we described in the second chapter. Companies must always stay abreast of the latest security technologies, as criminals are always finding new technologies and ways to carry out their crimes.

## References

Adeyoju FIP (2019) Cybercrime and cybersecurity: FinTech's greatest challenges. Available at SSRN 3486277

Al Duhaidahawi HMK, Zhang J, Abdulreza MS, Sebai M, Harjan SA (2020) Analysing the effects of FinTech variables on cybersecurity: evidence form Iraqi Banks. Int J Res Bus Soc Sci 9(6): 123–133

Al-Maksousy HHL (2018) Applying machine learning to advance cyber security: network based intrusion detection systems

Antonescu M, Birau R (2014) Financial and non-financial implications of cyber-crimes in emerging countries. In: International conference emerging markets queries in finance and business EMQFB, 3rd edn, 29–31 October 2014, Bucharest, Romania, published in Procedia - Economics and Finance (Elsevier Journals), vol 32, pp 618–621. https://doi.org/10.1016/S2212-5671(15)01440-9. https://www.worldbank.org/en/. The World Bank official website. Accessed on 10.5.2022

Arner DW, Barberis J, Buckley RP (2015) The evolution of Fintech: a new post-crisis paradigm. Geo J Int L 47:1271

Davis JJ (2017) Machine learning and feature engineering for computer network security. Thesis. https://eprints.qut.edu.au/106914/1/Jonathan_Davis_Thesis.pdf. Accessed on 9.5.2022

https://www.avast.com/c-cybercrime. Accessed on 1.5.2022

https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf. Accessed on 1.5.2022

https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. Accessed on 1.5.2022

Hughes SD (2017) Cryptocurrency regulations and enforcement in the US. W. St. UL Rev 45:1

Kang MJ, Kang JW (2016) Intrusion detection system using deep neural net-work for in-vehicle network security. PLoS One

Kasanda EN, Phiri J (2018) ATM Security: a case study of emerging threats. Int J Adv Stud Comput Sci Eng 7(10)

Kopp E, Kaffenberger L, Wilson C (2017) Cyber risk, market failures, and financial stability. International Monetary Fund

Leong K, Sung A (2018) FinTech (Financial Technology): what is it and how to use technologies to create business value in fintech way? Int J Innov Manage Technol 9(2):74–78

Medeiros M, Chau B (2016) Fintech-stake a patent claim? Intell Property J 28(3):303

Milne A (2016) Competition policy and the financial technology revolution in banking

Mohurle S, Patil M (2017) A brief study of wannacry threat: Ransomware attack 2017. Int J Adv Res Comput Sci 8(5):1938–1940

Najaf K, Mostafiz MI, Najaf R (2021) Fintech firms and banks sustainability: why does cybersecurity risk matter? Int J Financ Eng 8(02):2150019

Nikkel B (2020) Fintech forensics: criminal investigation and digital evidence in financial technologies. Forensic Sci Int: Dig Investig 33:200908

Ozili PK (2018) Impact of digital finance on financial inclusion and stability. Borsa Istanbul Rev 18(4):329–340

Pollari I (2016) The rise of Fintech opportunities and challenges. Jassa 3:15–21

Ramzan Z (2010) Phishing attacks and countermeasures. Handb Inf Commun Security:433–448

Rooney H, Aiken B, Rooney M (2017) Q. Is internal audit ready for blockchain? Technology Innovation. Manage Rev 7(10):41–44

Schatz D, Wall J, Schatz D, Wall J (2017) Security and law towards a more representative definition of cyber security towards a more representative definition of cyber security. J Dig Forensics
Schueffel P (2016) Taming the beast: a scientific definition of fintech. J Innov Manage 4(4):32–54
Spulbar C, Birau R, Calugaru T, Mehdiabadi A (2020) Considerations regarding FinTech and its multidimensional implications on financial systems. Revista de Sti-inte Politice 68:77–86
Stevens T (2018) Global cybersecurity: new directions in theory and methods. Politics and Governance. https://doi.org/10.17645/pag.v6i2.1569. Accessed on 9.5.2022.