Scientific Research Publishing

Beijing Law Review, 2025, 16(1), 29-57
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Prevention of Economic Crimes with the Help of Electronic Banking

Fereshteh Shademanpoor

Department of Law, Faculty of Public Law (International Law), University of Istanbul, Istanbul, Türkiye
Email: fshademan08@gmail.com

How to cite this paper: Shademanpoor, F. (2025). Prevention of Economic Crimes with the Help of Electronic Banking. *Beijing Law Review, 16,* 29-57.
https://doi.org/10.4236/blr.2025.161002

Received: November 13, 2024
Accepted: January 14, 2025
Published: January 17, 2025

Copyright © 2025 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution-NonCommercial International License (CC BY-NC 4.0).
http://creativecommons.org/licenses/by-nc/4.0/

Open Access

Abstract

Electronic banking represents an advanced form of traditional banking. In this system, all activities are conducted online, allowing for quick and remote transactions. In today's world, all countries need to adopt this modern banking approach and integrate their financial systems with digital technology. Moreover, economic relations between nations increasingly rely on the Internet and virtual platforms. As a result, countries inadvertently manage the majority of their financial and economic interactions through digital technologies. The electronic banking system plays a crucial role in detecting banking crimes effectively. One of the most concerning aspects of economic crimes is their transnational and organized nature. Such crimes can impact the economies of multiple countries, leading to significant monetary and financial challenges. Electronic banking, empowered by digital technologies such as artificial intelligence, can effectively help prevent and identify financial criminals. Unfortunately, some individuals may misuse these technologies to evade the law and gain illegal advantages. For instance, a skilled criminal could breach security measures to access personal and financial information from individuals and exploit it for their own benefit. This not only harms the victims but can also have detrimental effects on the overall health of the country's economic system. In this article, we highlight the significant role of electronic banking in detecting banking crimes and penalizing offenders.

Keywords

Electronic Banking, Economic Crimes, Money Laundering, Prevention of Financial Offenses

1. Introduction

In today's world, communication is closely tied to digital technology, which is

increasingly preferred across all scientific fields. Consequently, artificial intelligence and computer science have different affected on differently sciences. As a result, individuals who lack even basic knowledge of digital technology may feel anxious and confused in their daily lives and activities.

It seems that given the world around us, changes in the banking system have significantly transformed the global banking and financial industry. Modern banking now transcends national borders, making it possible for transactions to occur between countries, often facilitated by virtual networks and the Internet. In the past, before the Internet, transactions relied on a barter system, where goods were exchanged for other goods. Subsequently, cash transactions replaced these traditional methods, with cash being used to conduct commercial and banking services. Today, with the growth of the Internet, most transactions are conducted online, reducing the need for face-to-face interactions. All monetary and financial activities are monitored by the electronic banking systems of each country. This global connectivity and communication in the economic sector have made electronic banking a safe and effective platform for cross-border commercial and economic transactions. Recognizing the importance of this development, many countries have enacted laws to enhance the security and oversight of electronic banking systems. These laws, along with regular supervision of activities, enable individuals and institutions to conduct their financial operations in a secure and safe environment.

The key point is that while virtual spaces are cost-effective and well-suited for economic activities for individuals as well as private and governmental institutions and come with a high level of security, but unfortunately, in some instances, these environments can facilitate unauthorized activities by cybercriminals. Economic criminals can inflict significant damage on the banking and financial systems by compromising privacy in virtual networks and obtaining sensitive information from individuals. In some cases, these criminals are so skilled that they remain undetected.

The damage that a corrupt individual, such as a fraudster or embezzler, inflicts on a country's economic system can take years to repair. When there are disturbances in the banking system or when the financial and economic systems become compromised, it is the general population that suffers the most. This corruption creates a cycle of economic instability, leading to poverty replacing wealth, and ultimately, ordinary people become victims of this economic turmoil.

2. Electronic Banking

Electronic banking is a form of virtual banking that facilitates and speeds up financial transactions over the Internet. With electronic banking, customers can easily perform a variety of financial tasks, such as viewing previous transactions, making online purchases, processing remote payments, and transferring funds between bank accounts. It also allows users to manage bills and handle securities like checks and electronic promissory notes within the digital space, using advanced

technologies. This banking system, which can be accessed through online banking platforms or mobile applications provided by banks, saves time and reduces paperwork. It enhances the efficiency of services, speeds up customer support, and optimizes the overall banking experience. Additionally, electronic banking increases the security of account data, ensuring a safer transaction environment for users.

These transfers may sometimes encounter issues with banking transactions or internet and electronic financial transfers, leading to potential failures. However, since these transactions and financial activities are recorded in the bank as financial data, they can be tracked and compensated. For example, if funds are deposited into an institution's or individual's account through ATM machines but the intended money is not deposited into the destination account, it can be tracked through the bank. It is possible to receive legal compensation for losses and damages by referencing the provisions of the banking law in that country. This financial compensation from the bank involves specific steps and conditions.

The US Electronic Fund Transfer Act, 1978 provides that where a bank completely fails to make a credit transfer, or fails to make a timeout transfer, it is relieved from that liability if such failure was caused by an act of God or other circumstances beyond its control, or by a technical malfunction which was known to the customer at the time he/she attempted to initiate an electronic fund transfer (Kato, 2019: p. 106).

The development of technology in the banking sector has important implications for the marketing efforts of banks, particularly in Digital banks (DB) services as they affect customers' uses. DB over the phone, the Internet, and smartphones have become a major means of providing multi-channel services to customers, which is a challenge to the traditional banking models, as their use, retention, and improvement in profitability become important for digital banks. To re-engineer their marketing strategies to market their services and to accelerate the rate of adoption of digital banking. The wave of technological development has changed the face of the world in multiple economic sectors because banks are the mainstay of the economy with the increase in the volume of transactions in the global and local markets, as customers have also begun to prefer unconventional methods of banking services. So, it became delivered using IT tools anytime and anywhere without any direct participation from employees. Competition in the banking industry also grew too stiff levels and every effort was made to improve customer comfort by adding new channels and options for digital banking services. Because customer satisfaction is the only key to success, what the bank needs to understand their requirements is not an easy matter because the dynamics of digital and traditional banking are completely different (Sultan Altaie & Tayyeh Mohammed, 2020: p. 12398).

2.1. History of E-Banking

The foundations of banking services can be traced back to early civilizations such as Babylon and Sumer. Banking gained significant momentum after the Industrial

Revolution. Additionally, the influx of foreign investors and businessmen conducting their transactions through England played a crucial role in establishing England as a global financial center. During this time, banking practices in Europe and America underwent substantial improvements. After World War II, countries led by the United States began to engage more actively in international banking activities. The 1970s saw the advent of computer technologies, which banks integrated into their operations. This integration not only reduced transaction costs but also accelerated the services provided to customers. This era of globalization gained considerable traction, impacting countries economically, politically, culturally, and technologically. As the industrial age progressed, the world also entered the digital age (Akbaş, 2023: p. 2).

The developments in the banking system can be categorized into four distinct periods. In each era, computers and software have increasingly replaced both people and paper. Each evolution has enabled banking managers to minimize wasted time in a competitive environment and to expand the scope of their services. In summary, new technology and the digitalization of banking have allowed banks to enhance the speed, quality, accuracy, cost-effectiveness, and variety of their services. First Period: Automation Behind the Counter: This period marks the beginning of computer use in the banking system. Central computers were used primarily for processing information and paper documents produced in branches. These documents were collected in batches and sent to a central location for processing, usually at night. During this time, the main functions of computers were limited to bookkeeping and converting paper records into digital files. The automation of tasks behind the counter, which gained popularity in the 1960s, allowed banks to eliminate physical ledgers and cards from branches. Instead, the daily account transactions were sent to central computers at the end of each day for updating. By the 1970s, advancements in automation meant that branches no longer needed to send physical documents; instead, daily transactions were recorded on magnetic media and transmitted to central facilities. This information processing and account updating continued to occur within central computer rooms. The second period: Automation at the counter. This period began when branch employees started recording and processing banking operations electronically in the presence of customers. Since the late 1970s, continuous information transfer became possible through the use of terminals, which resembled today's personal computers, connected via telecommunication lines to large central computers. This advancement allowed for effective information exchange between vast computer networks and input/output terminals. During this time, branch employees gained continuous access to current accounts. To achieve front-of-the-counter automation, banks had to rely on existing telecommunication networks owned and monopolized by state-owned companies. However, these networks were not only limited in terms of technology but also expensive to use. These telecommunication and information networks connected the bank terminals in branches to the computer centers behind the counter. Despite the presence of

terminals, there was still a tendency to use paper documents. While the terminals facilitated searching and processing, all tasks were performed by bank employees who entered information and managed account circulation through the terminals. This reduced the reliance on paper to some extent. During this period, banks were able to reduce the number of employees, although there was still a need for personnel to manage client relationships. Additionally, the software used at this time remained unintegrated and isolated. The Third Period: Connecting Customers to Their Accounts. This period began in the mid-1980s and marked a significant advancement in customer access to their bank accounts. Customers could now access their accounts via telephone, ATMs, or personal computers using smart cards or magnetic cards. This allowed them to perform various transactions, such as receiving and making payments or transferring funds electronically. As a result, bank lobbies gradually emptied of long queues, allowing employees who previously handled customer transactions at the counters to be reassigned to other departments like marketing and customer service. Additionally, technologies such as satellites, microwaves, and wireless modems facilitated this transition and improved overall efficiency. The third period of banking evolution is marked by key features that set it apart from both the previous and subsequent periods. During this time, there was significant development in mechanized systems, both in front of the counter (for customer interaction) and behind the counter (for processing). Additionally, customer communication systems, such as ATMs, telephone banking, and mobile banking apps (like Fox Bank), began to emerge. Despite these advancements, human involvement remained essential in delivering services. In this period, bank cards and smart cards were not fully electronic in nature. Instead, there was a partial integration of electronic information exchange within banking operations, leading to a transitional phase that can be described as manual-electronic. The fourth period marks a significant advancement: the integration of systems that fully connect customers with all banking operations. This era begins when insights from the previous three periods are thoroughly addressed and their challenges resolved. In this phase, all banking operations are conducted electronically, allowing both banks and customers to access the information they need accurately and consistently. While the pace of these developments may vary, all four periods are expected to occur within the banking industry. To reach this stage, it is essential to have advanced and reliable telecommunications and communication platforms. This course provides a comprehensive summary of the software and hardware topics discussed in previous courses, effectively illustrating the relationship between the bank and its customers. In earlier periods, many banks operated in a disorganized manner, creating isolated mechanized systems instead of cohesive interactions (Mohaddes Khalasi, 2016: pp. 7-8).

2.2. Types of Electronic Banking

Electronic banking can be categorized into two main types: 1) Classification based on the nature of the bank providing dual banking services. This model includes a

combination of traditional banking and electronic banking methods. Traditional banks, which have physical branches (often referred to as "Brick and Click"), offer some or all of their banking services electronically to customers. In contrast, virtual banks provide all their banking services exclusively online and do not have any physical branches. 2) Classification based on remote service channels (electronic banking portals): Electronic banking refers to any tool that enables a bank to deliver its services to customers without the need for a physical branch and irrespective of time constraints. A broad range of electronic tools can be regarded as channels for electronic banking services. The most significant of these include banking through card readers and sales terminals, ATMs, internet banking, mobile banking, telephone banking, and bank kiosks (also known as VTMs) (Qashqai, 2022: pp. 3-4).

3. Electronic Economic Crimes

Economic crimes can be defined as criminal activities conducted by individuals or organizations that employ illegal methods to gain an unfair economic advantage. These crimes impact the economic system, and their effects can extend beyond borders, sometimes influencing the economic systems of other countries due to their cross-border and transnational nature.

Economic crime refers to acts committed for the purpose of achieving a financial advantage. It can also be defined as illegal activities carried out in professional settings to gain economic benefits (Forati, 2019: p. 67).

Before discussing electronic crimes, it's important to briefly explain economic crimes. Electronic economic crimes are essentially an evolved and modernized form of traditional economic crimes that existed before the development of digital technology and cyberspace.

Nicola Clough, a Swiss lawyer and criminologist, defines economic crime as a broad concept that encompasses a range of offenses damaging to the economic system or the framework of commercial and business relations within society. These crimes typically occur within the context of professional activities, often committed by companies or their management (referred to as corporate crimes). Based on this definition, economic crimes can be categorized into two main groups: 1) Economic Crimes Against Government Regulations: This category includes criminal activities that target the government economy, such as banking, markets, and competition, as well as the public budget—which covers taxes and customs—and the protection of consumers and the environment. 2) Crimes in the Field of Business and Commerce: This includes various offenses occurring in the business and commerce sectors, often perpetrated by professionals who violate laws governing commercial relations. Examples of these crimes include anti-competitive practices, abuse of trust, and violations related to goodwill (Sadegh Nejad Naini & Ebrahimi, 2015: p. 152).

In economic crimes, there is no violence involved; the primary goal is to achieve substantial illegal financial gains by violating laws and disregarding economic principles. The perpetrator, equipped with sufficient economic and financial

knowledge, exploits their position and legal resources to bypass economic regulations. A common example of economic crimes is white collar crime, which will be discussed in the following cases.

Defining economic crime comprehensively is challenging due to its similarity to other concepts, which creates obstacles in understanding. Economic crime is closely related to terms like financial corruption, economic corruption, and commercial crime, leading to some overlap between these categories. While economic corruption itself is not classified as a crime, it can serve as a criterion for identifying economic crime. In essence, economic corruption refers to behaviors that threaten a country's economic foundation, whereas economic crime encompasses actions that disrupt economic policies and activities. For example, the non-observance of regulations in the distribution of government services and facilities, as well as the misappropriation of government employees and officials, is considered economic corruption, especially when compared to the private sector. While some view financial crimes as a subset of economic crimes, the two concepts differ in terms of their nature and purpose. Financial crimes primarily involve violations against the government treasury, whereas economic crimes focus on the capital and property of private and public individuals. Examples of economic crimes include embezzlement and misappropriation in government transactions. In the context of economic crimes, the primary goal is to protect and sustain the economic system. This includes the structures involved in the production, distribution, and consumption of wealth. Examples of such crimes include money laundering and activities that disrupt a country's monetary or currency system. These offenses are addressed in laws designed to support economic activities, whether specified in economic crime legislation or in various regulations governing economic practices. Zlatrik defines economic crime as actions taken by legal or natural persons that pose a risk or inflict harm on a government's social or economic policy (Mirsaeidi & Zamani, 2013: pp. 170-168).

In the realm of electronic economic crimes, it is important to recognize that digital technologies have significantly accelerated individual financial crimes. These electronic economic crimes represent an evolved and modern form of traditional criminal activities. When victims engage in economic activities online and within virtual spaces for convenience, enhanced security, and faster transactions, they often place their trust in the internet, whether willingly or under compulsion. However, this trust is often misplaced due to insufficient security in cyberspace and a lack of awareness or knowledge among victims about protecting their personal information online. Criminals exploit this trust, leveraging the information they gather to perpetrate fraud and inflict substantial harm on their victims for significant financial gain. It is essential to note that victims of electronic economic crimes can include both individuals and legal entities or institutions.

3.1. History of Electronic Economic Crimes

Electronic economic crimes are a modern evolution of traditional economic

crimes; thus, a historical overview of these crimes will be presented first.

Many factors are effective in the occurrence of crimes. There is an extensive empirical literature, most of which includes studies that have been conducted in order to determine the effect of these elements, based on the conventional model developed by Becker. Fleischer's studies in 1963, in which he analyzed the effect of unemployment and income on juvenile delinquency, can be considered a pioneer in this matter. In Becker's model, which is accepted as a fundamental study in the relevant field, it is claimed that the criminal behavior of the individual emerges as a result of a rational choice. According to Becker, individuals engage in criminal behavior by comparing various factors: the potential income from committing a crime, the legal profits they could earn without breaking the law, the likelihood of being caught, and the financial consequences of any punishment. If individuals evaluate these elements and perceive that committing a crime is more profitable, they are likely to proceed with it. As the probability of arrest and punishment increases, the tendency of people to commit crimes decreases and people are discouraged from committing crimes. Ehrlich, who developed Becker's model by adding the time dimension, stated that people make decisions by comparing the benefits they obtain as a result of dividing their time between legal and illegal activities. Therefore, people turn to crime when the potential income opportunity they get from illegal activities is relatively more than the potential income opportunity they get from legal activities. The model referred to in the literature is known as the Becker-Ehrlich model. Following its development, there has been a significant increase in empirical studies conducted across different countries to test this model. These studies utilized panel data, cross-sectional data, and large datasets to explore the relationships between crime supply and various socio-economic and demographic variables. The study of the factors influencing crime encompasses various scientific disciplines, including economics, law, sociology, psychology, and geography. As a result, there are numerous factors that may contribute to an individual's tendency to commit crimes. Key elements include age, gender, education level, cultural characteristics, the judicial system, religious influences, physical and mental health disorders, family structure, genetic factors, social environment, poverty, unemployment, inequality, social exclusion, and population density. Additionally, research has shown that the physical environment can also impact crime rates. Some people believe that many prohibitions in Sharia, as outlined in the holy books, are linked to economic crimes. Pettigrew noted that scandals involving economic crimes, such as embezzlement and corruption by major colonial companies like the East India Company, the Royal African Company, and the Levant Company, caused significant harm to people in the 17th and 18th centuries. It is evident that these events prompted major changes in public administration. Criminologist Sutherland argues that the rate of economic crimes is significantly higher than that of other types of crimes when considering total crime rates. He points out the drawbacks of society's tolerant approach towards these offenses and emphasizes the comparison between economic

crimes and other criminal activities. Sutherland's research is also crucial because it demonstrates that economic crimes are not limited to individuals from lower-income or impoverished backgrounds; rather, they can also be committed by those in higher socioeconomic positions and with substantial wealth (Yildiz et al., 2022: pp. 254-256).

In his speech (Sutherland), at the American Sociological Association in 1939, Edwin Sutherland introduced the concept of white-collar crimes. He criticized his colleagues for their overemphasis on the crimes of lower-class individuals and the class prejudices that influenced their explanations of criminal behavior. This speech not only sparked increased research into white-collar crimes and their perpetrators but also initiated important discussions about the concept itself. Sutherland emphasized that a distinguishing feature of white-collar criminals is their respectable social position. His definition is centered on the characteristics of the perpetrators, highlighting their status and power in society (Ghorchi Beigi, 2018: p. 218).

An ideal environment for a variety of cybercrimes has been established by the growing usage of digital technology, including computers and the Internet. Unfortunately, there is no set date for the history of electronic economic crimes. However, it may be argued that during the 1990s, when the worldwide Internet became widely accessible to everyone, computer crimes have also emerged and increased in tandem. Economics, like other disciplines, has evolved with digital technologies as all sciences are intrinsically tied to the internet and digital world. The amazing thing is that, in the digital world and on the Internet, this advancement has two sides. Because, on the one hand, it is advantageous to integrate economic, financial, and banking issues with the Internet.

3.2. Types of Economic Crimes

The main categories of economic crime include: profiteering from ownership transformation processes, organized forms of tax crime, fuel market crime, illegal manufacturing, smuggling and trafficking of excisable products, money laundering-legalizing the proceeds of crime, use of banking institutions for illegal activities, insurance fraud, use of illegal electronic payment instruments, corrupt activities. These are just a few examples of criminal activities emerging in the area of economic turnover. Nowadays, new areas of their activity are emerging, and it is also becoming common for a single criminal group to undertake activities from different areas of criminal interest, the so-called multi-criminal groups. On the basis of Polish literature, as early as in 2009, Jaroch drew attention to the structure of economic crime, stating that for years economic fraud has dominated (over 30%). Apart from economic fraud, the next category is economic falsification (at 15%), followed by crimes against economic turnover (here we can observe a decrease in the share in the structure from 14.5% to approx. 7%) and crimes against intellectual and industrial property (an increase from 6.8% to 10.2%). This is a certain trend that characterizes the structure of crime in the world: misappropriation of assets, fraud, piracy and counterfeiting, corruption and falsification of

financial data, money laundering, and insider trading in shares. It is important to bear in mind that the phenomenon of economic crime is evolving all the time and can take on different dimensions in specific economic areas, depending on their development (Jakubiec & Kuliński, 2023: p. 57).

In the following sections, we will discuss the most frequent topics about economic crimes, emphasizing the electronic element of those crimes.

3.2.1. Electronic Money Laundering

It is necessary to provide a brief explanation of the simple type of this crime before entering into the subject of electronic money laundering.

In a simple definition, Money Laundering is the conversion of profits from criminal and illegal activities into apparently legal and legitimate funds. In the process of money laundering, the money resulting from illegitimate and illegal actions becomes an asset or finance, which is apparently obtained through legal and correct means, and in this way, the laundered money enters the economic cycle.

Money laundering is the processing of proceeds from criminal activities in order to hide or change the appearance of its illegal origin. In the context of fighting money laundering, this phenomena is defined as follows in international agreements, rules, and regulations compiled in various countries: According to the European Community's guidelines, which were approved in March 1990, money laundering is defined as the conversion or transfer of property while knowing that it was obtained through criminal activity in order to hide or eliminate evidence of its illegal origin or to assist someone who is committing such a crime. The International Criminal Police Organization has defined money laundering as any act or attempt to act that conceals or modifies the appearance of the identity of a person in order to evade legal repercussions. The definition of money laundering was completed in the Treaty of the Council of Europe, related to the meeting of August 1990, Strasbourg 3 and the following items were added to the definition presented in the action order of the European Community: acquisition, possession, or use of assets obtained from illegal sources and also Any participation, supervision, conspiracy to commit, attempt to commit or assist, encourage, facilitate and conceal any crime related to money laundering. Some people might believe that money laundering entails giving legitimacy to illegal funds; for instance, by taking someone else's money and using it to satisfy the owner. Although this is a positive thing, money laundering actually means that illicitly obtained dirty money is introduced into transactions, bank transfers, and other financial transactions as legal assets in the exchange of the economy of society and in the activities of individuals (Farkhondeh et al., 2023: p. 477).

In the distant past, criminals typically did not use their ill-gotten gains openly. As a result, there is no consensus on when the term money laundering was first used or its widespread acceptance among researchers. It is believed that the modern concept of money laundering first emerged in 1979 when a suitcase containing six hundred million dollars in cash was discovered at Palermo Airport, which was

linked to drug sales. This incident contributed to the establishment of the Italian-American Pizza Connection case, with a trial held in 1985. The term is also thought to have originated from the mafia's involvement with coin-operated laundry machines in America. During the 1920s, gangsters amassed large sums of cash through activities such as extortion, prostitution, gambling, smuggling, and bootlegging. They needed a way to disguise the sources of their illegal funds. One common method was to purchase legitimate businesses and mix their unlawful revenue with the legal income generated from these enterprises. Coin-operated laundries were particularly appealing because they generated a substantial amount of cash daily without raising suspicion. The term "money laundering" first appeared in the press during the Watergate scandal in 1973, and by 1982, it began to be included in American judicial and legal texts (Nasiri, 2016: p. 2).

Black money, refers to the financial gains derived from activities that are deemed illegal under the law. A criminal faces risks unless they can effectively conceal the source of their illicit profits or create the illusion that these funds were acquired through legal means. This is critical because there is a possibility of criminal prosecution and confiscation of these gains, stemming from the crime that generated the profit. In countries with a free market economy that also maintain strict and effective controls on the financial system, the use of cash is typically low. As a result, large cash transactions raise red flags, prompting scrutiny of the asset's origin. To avoid detection, criminals must sever the connection between their illegal activities and the profits they earn, ensuring that these profits appear to be legally obtained (Coşkun, 2004: p. 230).

In order to provide a comprehensive definition of crime, the characteristics of the crime must be examined. Below are brief characteristics of this crime.

The crime of money laundering is characterized by characteristics that differ from traditional crimes, and it is similar in most of these characteristics to the characteristics of organized crime, such as arms trafficking and smuggling, counterfeiting, terrorism, and other crimes. The characteristics of the money laundering crime are as follows: 1) Complementarity, comprehensiveness, and connection, as this crime is considered one of the crimes with close connection between its components, as it must have integrated elements, each part complementing the other, starting from the depositing stage, then the coverage stage, and ending with the integration stage. 2) It is subject to the elements of organization, planning, control, and performing roles with precision, skill, and mastery, and there is no room for improvisation. 3) It is considered one of the crimes whose occurrence it is useful to prevent preventive measures, so that all means and methods must be followed that dry up the sources of this crime before it occurs and significantly limit its impact afterward. 4) The communications revolution and advanced information technology and their use in banking and financial operations have given global and international features and dimensions to the crime of money laundering, as it has become borderless and cross-continental, and does not stop at the geography of a specific country, this renders the local national efforts

insufficient to confront this phenomenon with its various aspects and dimensions, and no country can consider itself immune to the challenges and dangers of this phenomenon. 5) The crime of money laundering is an intentional crime, extending to anyone who possesses, owns, benefits, assists, contributes, mediates or intervenes in any stage of this crime, provided that the elements (intention, intent) and knowledge are present, whether this was done by people or banking or financial institutions, which contributes to concealing the source of the laundered money or intended to be laundered (Mustafa Ali & Edris Mohammed, 2023: p. 197).

These stages/phases that are not always easily distinguished, but may take place in sequence or simultaneously, are the following: 1) Placement: Dirty money accumulates in large quantities of banknotes, which are extremely difficult to transport physically. After all, while dirty money is still liquid, it is exposed to the risk of "theft" or "embezzlement." For these reasons, the immediate priority of the interested parties is to channel the dirty money into the legal financial system of the country or abroad by converting it into the usual forms of financial values. In the first stage, criminals try to place illicit funds inside the financial system. This is achieved by "breaking up the large amounts of cash into less conspicuous and smaller sums" that are inserted into the banking system through deposits and wire transfers. Besides that method, which is known as smurfing, placement of illicit funds is also pursued through bribery of bank employees or through blackmail. The sub-banking sector (e.g. foreign exchange offices) is also used to launder money. Additionally, for the same purpose, many times "dirty cash" is transferred to offshore financial centers. Placement of illicit proceeds in the real market through endless methods like the purchase of expensive goods which are then sold again or through other means such as the abovementioned deposits in casinos is also probable. 2) Layering: The second step involves the transfer of funds throughout more than one financial system across jurisdictions, usually through complex trades. This is the case of wiring funds to offshore "shell" companies that has been explained in the previous section. That step aims to conceal the owner of the illicit funds through the inherent complexity and secrecy that these kinds of legal entities offer to their controlling parties. 3) Integration: This is the last step in the process of money laundering. In this stage, "dirty money" returns to the country of origin, to take the form of legal funds and investments. The real owner of the money can appear as such since the money cannot be detected as illegal. Consequently, he spends it in new criminal activity or investments in legitimate businesses that support organized crime (Valvi, 2023: p. 34).

By examining the aforementioned cases, we can conclude that money laundering involves an organized and coherent system or institution, along with skilled professionals who operate with seriousness and expertise, such as hackers in cyberspace. Responsibilities are assigned based on a detailed, complex, and confidential structure. This requires a network, or even multiple organized networks, characterized by a high degree of professionalism, coordination, planning, and

global reach. Money laundering is a complicated and sensitive issue because it seeks to create a false reality that appears true and legitimate. The primary objective is to transform the cash flow from illegal activities into other forms of assets, thereby ensuring the continuation of illegal financial gains. This allows for the use or investment of these funds in legitimate activities without attracting suspicion or risking confiscation by government authorities and security services.

Money laundering has harmful consequences for countries and the world community. Money laundering, as a transnational organized crime, can bring the domestic economy of a country to the abyss of destruction, and can also cause unhealthy economic relations of countries in the world arena. Increasing domestic inflation and liquidity, reducing productivity in the domestic and international economic sector, disrupting the countries financial and banking system, weakening the private sector, devaluation of the national currency, tax evasion and thousands of other problems, all due to the existence of money laundering. Have been realized and causes a crisis in a healthy economy.

In the past decade, advancements in digital technology have significantly impacted banking and economic activities, leading to an increase in remote transactions conducted online. As this technology continues to grow and intertwine with various economic aspects, it has provided opportunities for economic criminals to exploit the system. These criminals can now commit acts of fraud more easily and quickly, driven by the desire for illegal profit through various methods in cyberspace. Consequently, money laundering can be categorized into two types: traditional and modern (electronic).

Before the rise of digital currencies, money laundering with fiat currencies typically involved criminals creating several bank accounts and moving their money among these accounts under various titles. To establish each of these accounts, criminals had to go through an authentication process and provide their identity information to the bank. In this traditional system, money transfers were strictly controlled by central banks. In contrast, transferring digital currencies requires only the wallet address of the other party. Digital currency transactions are not overseen by any central authority or intermediary. However, to convert digital currencies back into fiat money, users must rely on a digital currency exchange. To combat money laundering through digital currencies, many exchanges require users to authenticate their identities. Most of the world's major exchanges, which handle a high volume of transactions, mandate user authentication. Still, some smaller exchanges do not have such authentication requirements (Moradi Ghale, 2013: p. 272).

The question raised in this section is; are there departments that monitor digital currency transactions?

Many central banks around the world have accelerated their efforts to minimize the potential risks that the digitalization process may pose to traditional payment systems and to stay ahead of current developments. The report published on March 13, 2023, by Juniper Research, which operates in the FinTech, and

payments markets, includes the expectation that significant progress will be made in the future for CBDCs. According to the related report, the value of payments made through CBDCs in 2023 is only 100 million dollars, and this value is expected to reach 213 billion dollars annually by 2030. The current situation shows that it is highly likely that the number of studies conducted to research and test CBDCs will increase and that the use of CBDCs will become widespread in this context. The widespread use of CBDCs prevents the central banks of countries from being indifferent to the relevant digital currency and determines their attitude toward CBDCs. However, it should be noted here that each country's CBDC has different characteristics, serves different purposes, and is shaped according to the conditions of the country. Therefore, a single CBDC design is not possible, and central banks should design CBDCs with the most appropriate structure for their countries to eliminate the potential risks that they may pose. In this context, countries in various income groups try to have as much information as possible about the transition to CBDCs and the post-transition process and to follow current developments closely. For instance, as seen from the IMF (2023) report, more than 40 countries have requested IMF assistance in CBDC capacity building, and the IMF has developed various recommendations. In addition, the IMF has announced that a CBDC handbook will be developed to concretize and compile the results of its work on CBDCs. It is expected that this handbook may be an important source of reference for policymakers, especially in developing countries, and that it will make an important contribution to countries in determining whether they have a suitable structure for them. As is known, CBDCs are expected to provide benefits in many areas, such as encouraging financial inclusion, reducing transaction costs, increasing the efficiency of payment systems and the stability of monetary and fiscal policies, and preventing informality. On the other hand, decentralization, money laundering, a lack of confidentiality and infrastructure are among the major risks that CBDCs may pose. In this respect, first of all, the rule-making and enforcement functions of regulatory and supervisory agencies should be enhanced in order for the central banks of the countries to benefit from these advantages to the maximum extent, to rule out potential risks, and to establish a sound CBDC system. Therefore, the central bank of each country willing to issue CBDCs should cooperate with these institutions and adopt a conscious attitude to prevent possible money laundering, etc., attempts. In addition, countries should meticulously analyze their sociodemographic structures in detail and accurately identify the needs of potential parties that may have difficulties adapting to the CBDC system. Only then will it be possible to expand financial inclusion, one of the key benefits of CBDCs. It is also crucial for CBDCs, which are seen as a new financial oversight tool, that countries create their own technical infrastructure systems with a focus on preventing cyber-attacks. This study may contribute to a better understanding of a digital currency with such high development potential by both official authorities and individuals as potential users and to increase awareness of this issue. In future studies to be conducted on this subject, it

would be beneficial to consider countries on an individual basis and to make evaluations on a more micro basis by taking into account the effects of the relevant digital currency on the economic environments of the countries, monetary policies, and the attitudes of the citizens of the country toward this currency, and to develop the necessary suggestions, if any (Ceylan, 2024: p. 583).

For the effective operation of a Central Bank Digital Currency (CBDC) system, countries must ensure that their internet networks are strong and have wide coverage. Additionally, the system needs to be safeguarded against cyber-attacks, interruptions in data transmission, technical failures, fraud risks, and faulty algorithms. If these aspects are not adequately addressed, the system may malfunction and create opportunities for money launderers, terrorist financiers, and fraudsters. Given that the current conditions of countries vary significantly and existing regulatory frameworks are fragmented, there is a substantial need for global cooperation. This includes sharing best practices and harmonizing policies. Developed countries with ample human and financial resources may have an advantage in this area. However, developing and poorer countries can only seize these opportunities if their governments demonstrate commitment and secure sufficient external support. If developing countries effectively manage the transition to the CBDC system and its implementation, they may experience faster development and increased chances of catching up with developed nations. Conversely, if not managed well, the development gap between richer and poorer countries could widen. The success of the transition to the CBDC system and its continued operation also depends on the cooperation of relevant national and international organizations. Enhanced collaboration among these entities can lead to improved economic conditions and opportunities for countries. The CBDC system can be protected against cyber-attacks through the use of block chain technology or other advanced methods, similar to those used in the Bit coin system. Unlike crypto currencies, which lack state affiliation and guarantees, damages incurred from cyber-attacks in the CBDC system can be compensated by the state—provided the security measures put in place are effective, and losses are not due to user negligence (Demir & Odabaşi, 2022: pp. 218-219).

In order to increase supervision, better control and clarify financial affairs regarding money laundering, the banking system should be inspired and helped.

The AI algorithms implement predictive and other pre-defined binary rules to automatically analyze transactions' input and output. This enables an AI system to recognize any anomalies in the data provided, which flags and helps pre-vent financial fraud. Additionally, scientists continually find ways to improve algorithms' accuracy and reliability, reducing false alerts as they analyze records more carefully. AML solutions implemented in banks have a linear pipeline workflow that links with the data source. Data analysts and programmers then add certain parameters that help identify risky transactions, customers, or communications that might indicate fraudulent behavior. A typical AML system consists of four layers: a data layer, a screening and monitoring layer, an alert and event layer, and

an operational layer. The banking system relies on credible information provided by customers to monitor legitimate and suspicious activities. Therefore, the data layer is concerned with the collection, management, and storage of data. Financial institutions with effective AML systems do not solely rely on internal and employee data because they also obtain information from fraud watch lists and regulatory authorities. The data records are then analyzed using different AI and machine learning techniques natural language processing that improves the capability of computers to read, understand, and derive meaning from human languages and insights that help link relationships between clients and transactions. The screening and monitoring layer analyzes clients and transactions for suspicious activities. This stage is automated, and it implements certain rule-based techniques this technique is to capture the expert skills of a specialized human and to incorporate them into a computer system and risk analysis approaches. Rule-based systems have pre-defined parameters and thresholds used to identify launderers. The AI systems need not be too strict, which could lead to multiple false alerts, or insufficiently strict, which could allow illicit transactions to occur. This layer obtains user information stored in the data layer to screen customers and transactions. Whenever suspicious activity is identified, the alert and event layer raises the alarm, indicating the occurrence of a suspected transaction. A human operator then reviews the raised issues and takes the appropriate actions, including allowing, rejecting, or blocking the transaction manually. The manual operations of reviewing the transactions might overwhelm human operators, especially when a system reveals too many false positives the issue of many false alerts is resolved using a combination of AI and data mining techniques. One approach followed is outlier detection for fraud or laundering identification. In this approach, researchers define various parameters of a peer group by analyzing its transaction habits. Hundreds of thousands of records spanning several months to years are needed to classify data into different clusters or groups. Such data are effective because they capture the similarities and differences in grouping transactions with the highest similarity index to one cluster. The accounts or transactions in one cluster are similar, and they are different from other clusters. The benefit of this approach is that it helps group riskier accounts and transactions together. Additionally, because money laundering techniques evolve with time, AI can identify outliers and be-havioral pattern changes. Therefore, AI and machine learning techniques can identify suspicious transactions or irregular networks of money transfers not defined within the outlier parameters (Alhajeri & Alhashem, 2023: pp. 292-293).

By addressing the points mentioned above, it is crucial to utilize artificial intelligence in financial centers to enhance business and commercial activities aimed at detecting and preventing financial crimes such as money laundering and fraud. By implementing machine learning algorithms, financial institutions can categorize customers and transactions into low-risk and high-risk groups, enabling them to automatically analyze transaction data for anomalies and prevent fraudulent

activities. Consequently, this approach will help maintain the integrity of the global economy and improve security by identifying and intercepting the substantial amounts of money that are laundered each year.

Data alone cannot be used, but the knowledge hidden in the data can be used. Therefore, money laundering cannot be uncovered without an intelligent and data-driven tool. Data mining is a solution to this problem that helps use the knowledge hidden in data and provides the ability to predict and estimate suspicious money laundering activities. For this purpose, banks use AML anti-money laundering software and use it to analyze data and identify suspicious transactions. This software classifies customer account data based on the deviations that their accounts show. These deviations include withdrawals of large amounts or sudden increases in bank deposits. Another issue that can be examined in electronic banking is how to authenticate and register the national code in the banking system; because some people may commit money laundering by opening multiple accounts. Limiting the number of accounts for individuals is one of the preventive factors. Also, among the accounts used in money laundering activities are accounts that are invalid despite their identification numbers. In these accounts, the person whose details are registered with the bank is not the user of the account. These accounts were probably opened either with the deliberate cooperation of bank employees or by people skillfully opening accounts in other people's names using lost or stolen national identification cards (Hosseini & Azari Matin, 2016: pp. 141-142).

In this section, the question comes to mind: How does electronic banking affect financial crimes?

Carbon Banking is a software solution that stores all financial information and transactions in a given banking network in a central database (Core). This solution is used to accelerate and improve banking operations, reduce costs, and prepare for the growth of bank services. Accessibility, integration, and security are important features of Carbon Banking (https://www.dotin.ir).

The banking system can easily control and monitor all transactions. Machine monitoring methods based on artificial intelligence are much more reliable and secure than human monitoring methods. Because humans may make mistakes or omissions, while machine errors are very rare when it comes to monitoring banking transactions.

Another question raised is: What measures should be taken to ensure data security in electronic banking?

Threats to an electronic system can be caused by duplicating devices, changing or duplicating software information, changing sent messages, stealing hardware or software information, and causing it to malfunction. Attacks that can cause damage include malware, viruses, worms, trojan horses, backdoors, keyloggers, security holes, eavesdropping, Phishing, Pharming, Skimming, and poofing attacks. Therefore, there must be a mechanism to guarantee the completion of every banking transaction in which sensitive financial data is exchanged. To achieve this

important goal, methods such as using passwords, applying encryption mechanisms, and using signatures and security protocols are used (Hemmati, 2011: p. 3).

Dr. David Chaum, CEO of DigiCash said that "Security is simply the protection of interests. People want to protect their own money and banks their own exposure. The role of government is to maintain the integrity of and confidence in the whole system. With electronic cash, just as with paper cash today, it will be the responsibility of government to protect against systemic risk. This is a serious role that cannot be left to the micro-economic interests of commercial organizations." The security of information may be one of the biggest concerns to the Internet users. For electronic banking users who most likely connect to the Internet via dial-up modem, is faced with a smaller risk of someone breaking into their computers. Only organizations such as banks with dedicated Internet connections face the risk of someone from the Internet gaining unauthorized access to their computer or network. However, the electronic banking system users still face the security risks with unauthorized access into their banking accounts. Moreover, the electronic banking system users also concern about non-repudiability which requires a reliable identification of both the sender and the receiver of on-line transactions. Non-secure electronic transaction can be altered to change the apparent sender. Therefore, it is extremely important to build in non-repudiability which means that the identity of both the sender and the receiver can be attested to by a trusted third party who holds the identity certificates. Software-Based Systems In software-based security systems, the coding and decoding of information is done using specialized security software. Due to the easy portability and ease of distribution through networks, software-based systems are more abundant in the market. Encryption is the main method used in these software-based security system. Encryption is a process that modifies information in a way that makes it unreadable until the exact same process is reversed. In general, there are two types of encryption. The first one is the conventional encryption schemes, one key is used by two parties to both encrypt and decrypt the information. Once the secret key is entered, the information looks like a meaningless jumble of random characters. The file can only be viewed once it has been decrypted using the exact same key. The second type of encryption is known as public key encryption. In this method, there are two different keys held by the user: a public key and a private key. These two keys are not interchangeable but they are complementary to each other, meaning that they exists in pairs. Therefore, the public keys can be made public knowledge, and posted in a database somewhere. Anyone who wants to send a message to a person can encrypt the message with the recipient public key and this message can only be decrypted with the complementary private key. Thus, nobody but the intended receiver can decrypt the message. The private key remains on one's personal computer and cannot be transferred via the Internet. This key is encrypted to protect it from hackers breaking into the personal computer. There are four examples of current encryption technology presented below: Digital Signature,

Secure Electronic Transaction, Pretty Good Privacy, and Kerberos. 1) Digital Signature. 2) Secure Electronic Transaction (SET). 3) Pretty Good Privacy (PGP). 4) Kerberos (Yang, 1997: pp. 5-6).

Regarding laws to combat financial crimes in electronic banking, it should be acknowledged that most countries (especially countries with free and advanced economies) have developed a series of rules and principles in their local and national laws. But we will briefly mention some of these rules.

The Electronic Signatures Act 2010: This is aimed at making provisions for and to regulate the use of electronic signatures and provide for other related matters. Electronic Signature means data in electronic fonn affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message and includes an advance electronic signature and the secure signature (Charles, 2013: p. 37).

Many countries, such as the United States and Uganda, follow this rule.

Bank Secrecy Act (BSA): The OCC prescribes regulations, conducts supervisory activities and, when necessary, takes enforcement actions to ensure that national banks have the necessary controls in place and provide the requisite notices to law enforcement to deter and detect money laundering, terrorist financing and other criminal acts and the misuse of our nation's financial institutions (https://www.occ.treas.gov).

Due to the automated and electronic nature of the banking system, all countries are legally required to anticipate and prepare for potential issues. An effective law must be established that not only prevents similar crimes but also includes disciplinary measures for enforcing punishment and ensures proper implementation.

The delay in the possible abuses of recognition of new technologies and main modifications is one of the obstacles to the national criminal law and the legal system. These obstacles are still relevant. In addition, they are also topical as the speed of the acceleration of the network innovation:

1) Adjusting the national law to recognize the new technology abuse.

2) Identifying gaps in the penal code ensuring the valid legislative foundations.

3) Drafting of new legislation.

Although many countries have enacted new laws fighting cybercrime starting with the United States of America in 1978 and expanding to most countries including Arab countries such as Saudi Arabia and the United Arab Emirates, they are incompatible with local character and contain legal gaps. Therefore, it is necessary to establish effective international laws according to the information and databases of graphic information specific to this aspect (Rashid et al., 2021: p. 9).

More than anything else, countries should agree on international agreements to prevent financial crimes through electronic banking.

In some instances, certain countries prioritize their national laws over international law. This tendency, particularly in cases involving financial crimes, often leads to violations of international law that are neither rational nor justifiable.

Such actions disrupt the economic balance between two or more nations. Therefore, any country that, for any reason, violates the terms of a legal agreement should be held accountable and face penalties, without any concessions or leniency.

3.2.2. Electronic Fraud

The crime of traditional fraud is: taking another's property, by resorting to fraudulent means or operations.

Fraud has become increasingly prevalent in today's society, influenced by changes in the business environment and a growing tendency towards extravagance. The crime of fraud was first mentioned as a distinct offense in the French Penal Code of 1791. Sociological research indicates that various factors have contributed to the expansion of fraud, including the rise of communication tools, transformations in industry and trade, remarkable scientific discoveries, accelerated production of goods, and increases in the value of money. As a result of these influences and the fraudulent desires of individuals, the number of perpetrators has significantly risen. In fraud cases, the will of the victim is often compromised by the deceptive actions of the fraudster (Korkmaz, 2020: pp. 1416-1417).

With the digitization of financial and banking activities, most fraud occurs in cyberspace and within the digital realm of banks. A hacker can obtain all of a victim's information with just one click and exploit that information for personal gain. In fact, virtual platforms provide the easiest means for individuals with malicious intent to abuse the system and acquire unauthorized benefits.

Around 65% of the total fraud cases reported by banks were technology-related frauds (covering frauds committed through, at an internet banking channel, ATMs and other payment channels like credit, debit & prepaid cards) whereas advance-related fraud accounted for a major proportion of involved in fraud. 1) Triangulation cloning: Customers enter their card details on fraudulent shopping sites. These details are then misused. 2) Hacking: Hackers or fraudsters obtain unauthorized access to the card management platform of banking system. Counterfeit cards are then issued for the purpose of money laundering. 3) Online fraud: Card information is stolen at the time of an online transaction. Fraudsters then use the card information to make online purchases or assume an individual's identity. 4) Lost or stolen card: It refers to the use of a card lost by a legitimate account holder for unauthorized and illegal purposes. 5) Debit card skimming: A machine or camera is installed at an ATM in order to pick up card information and PIN numbers when customers use their cards. 6) ATM fraud: A fraudster acquires a customer's card, PIN and withdraws money from the machine. 7) Social Engineering: A thief can convince an employee that he is supposed to be let into the office building, or he can convince someone over the phone or via e-mail that he's supposed to receive certain information. 8) Dumpster diving: Employees who aren't careful when throwing away papers containing sensitive information may make secret data available to those who check the company's trash. 9) False pretenses: Someone with the intent to steal corporate information can get a job with

a cleaning company or other vendor specifically to gain legitimate access to the office building. 10) Computer viruses: With every click on the internet, a company's systems are open to the risk of being infected with nefarious software that is set up to harvest information from the company servers (Digamberrao Gudup, 2016: p. 214).

Phishing is one of the financial crimes that have become widespread in many countries.

Criminals using this method first create a fake webpage that closely resembles the official page of a bank. They use this fraudulent page to collect sensitive information, such as the card number, the second password, and the CVV code. At a strategic time, they then withdraw funds from the victim's account. To avoid raising suspicion, these criminals often display a message claiming that the bank's system is temporarily disconnected, which helps gain the trust of the user. Sometimes, after acquiring the individual's information, they even log into the bank's official website (Najafi Tawana & Karimi, 2021: p. 421).

3.2.3. Financial Fraud (Embezzlement)

Embezzlement is the act of illegally taking or misusing assets belonging to an individual, organization, or company. It typically involves unauthorized access to and theft of money or property. Embezzlement falls under the category of financial crimes and often occurs in environments where there is a lack of transparency in the banking system.

Typically, an embezzler abuses the trust placed in them by an institution or organization due to their job responsibilities. This betrayal can severely damage the organization's financial system in a very short period of time. Since they possess in-depth knowledge and a professional background, embezzlers are often well-equipped to commit financial crimes.

Article 22 of the United Nations Convention Against Corruption stipulates that all member states must implement legislative measures and other necessary actions to criminalize the intentional act of embezzlement committed by managers or employees of private sector organizations during economic, financial, or commercial activities. Embezzlement in this context includes private funds, government securities, or any other property entrusted to an individual due to their position. This article indicates that there is no distinction between the responsibilities of financial officers in private and public institutions. Importantly, the responsibility for managing financial affairs lies with the custodian. In simpler terms, individuals in either a public or private institution are tasked with supervising or safeguarding the property belonging to that institution. The expectation of accountability for any violations is clear in all situations. The person in charge must be prepared to answer for any financial crimes that occur within their scope of responsibility.

One of the Egyptian lawyers discusses the elements of the crime of embezzlement. This crime consists of five key elements: the nature of the perpetrator, the act of embezzlement itself, the type of embezzled objects, the transfer of these

objects as part of a duty, and the presence of criminal intent. It is essential for the perpetrator, referred to as "Machala's", to be a public employee or someone under the government's authority. This category includes employees of both central and local government, presidents and members of parliament, members of the armed forces, and anyone entrusted with a specific government role, as well as individuals working in public services (Aghababaei, 2007: p. 131).

Many abstract business transactions are based on a considerable amount of trust that the individual will play the rules of the game or respect the "folkways" of the business world. There are short cuts in the prevailing financial communicate tons which yield economic profit as long as the institutions of social control can be deceived. These opportunities are not restricted to trustees in advanced positions only. In the form of any simple confidence game or as an installment fraud, for example, they are open to any citizen of average intelligence. If, nevertheless, embezzlement is more restricted to trustees of one kind or another, this is due only to two circumstances: 1) higher temptation inasmuch as the financial gains thus obtained more adequately balance the risks involved; and 2) necessary expert skill in anticipating and counteracting the discovery by protective institutions (Riemer, 1942: p. 411).

4. The Impact of Clarification in Electronic Banking on Economic Crimes

With the help of digital technologies, the banking system has made significant progress in combating financial crimes and apprehending criminals. In today's banking environment, data is organized and defined within computer systems and banking networks. Once this data is established, the system is capable of reporting even the smallest errors or inconsistencies. As a result, human intervention is no longer necessary for identifying offenders, as digital technology now plays a crucial role in monitoring activities in the virtual space. It is important to note that all banks, both private and public, operate under the supervision of the central banking system and are officially managed and regulated by the central bank. This enhances the effectiveness of electronic banking in addressing economic crimes.

Block chain is a technology used for storing information in a distributed and immutable format within blocks. In today's modern banking industry, it has proven to be highly beneficial. It helps streamline financial transactions, enhances security, verifies customer identities, and supports the provision of technology-based banking services.

When data on a block chain is accessed or altered, the record is stored in a "block" alongside the records of other transactions. Stored transactions are encrypted via unique, unchangeable hashes. New data blocks don't overwrite old ones; they are "chained" together so any changes can be monitored. These blocks of encrypted data are permanently "chained" to one another, and transactions are recorded sequentially and indefinitely, creating a perfect audit history that allows visibility into past versions of the block chain. When new data is added to the

network, the majority of nodes must verify and confirm the legitimacy of the new data based on permissions or economic incentives, also known as consensus mechanisms. When a consensus is reached, a new block is created and attached to the chain. All nodes are then updated to reflect the block chain ledger. In a public block chain network, the first node to credibly prove the legitimacy of a transaction receives an economic incentive. This process is called "mining. "Here's a theoretical example to help illustrate how block chain works. Imagine that someone is looking to buy a concert ticket on the resale market. This person has been scammed before by someone selling a fake ticket, so she decides to try one of the blocks chain-enabled decentralized ticket exchange websites that have been created in the past few years. On these sites, every ticket is assigned a unique, immutable, and verifiable identity that is tied to a real person. Before the concertgoer purchases her ticket, the majority of the nodes on the network validate the seller's credentials, ensuring that the ticket is in fact real. She buys her ticket and enjoys the concert (Carson, 2024: pp. 2-3).

Today, various countries have developed software to monitor micro-information online, meaning that every transaction, action, and decision should be conducted digitally. The key distinction between post-preparation supervision of financial statements and supervision during operations is that during operational supervision, the central bank holds complete authority over any violations. In a transparent system, every citizen is required to provide a self-declaration. Furthermore, in the guidance, control, and monitoring framework, all data must be recorded and tracked. There is no need for military, security, or law enforcement agencies to oversee banks; instead, a mechanized banking system can actively prevent corruption and eliminate unauthorized and illegal access. This approach involves the internal monitoring of banks using scientific and systematic methods. Internal banking supervision can effectively combat organized corruption and assist the judiciary in this regard. The introduction of new technologies into the banking system and the implementation of electronic government can help prevent organized corruption. Banks should prioritize the collection of both large and small claims. Economic corruption is not confined to any single sector; rather, all institutions must work together in a coordinated effort to combat it. When embezzlement occurs in a bank, it poses a threat that extends beyond the bank's capital, jeopardizing the entire financial system of the country. Any loss of trust in the banking network can lead to a recession and financial crisis. All forms of economic corruption—whether public or private, including bribery, abuse of office, and embezzlement—are serious issues that can be found in every society, both developed and developing. However, the negative effects are often more pronounced in developing nations. In many of these societies, corruption incurs substantial economic costs. It disrupts the functioning of free markets, slows economic development, and hampers the ability of institutions and bureaucracies to provide essential services to citizens. Additionally, corruption adversely affects efforts to combat poverty (Azizi, 2020: p. 2).

When transparency is enhanced through digital technology, it fosters widespread trust and confidence in financial and banking matters. Financial managers increasingly recognize their responsibility to the public. In managing banking affairs, an impartial authority oversees all financial transactions and banking activities, ensuring that even the smallest discrepancies are reported.

4.1. Prevention of Economic Crimes

In 1981, the Council of Europe urged member states to pay special attention to preventing economic crimes. In line with this, the Law on Combating Smuggling of Goods and Currency, approved in 1392, uses the term "combat" to frame these offenses as adversarial. After providing definitions, examples, and organizations in its first chapter, the law shifts focus. Unlike the United Nations Convention on combating corruption, which emphasizes punitive measures, this law prioritizes prevention. Following the Law on the Punishment of Arms, Ammunition, and Owners of Illegal Weapons, approved in 2010 (Article 19), a separate chapter—Article 11—was dedicated to the prevention of smuggling. It strongly conveyed the message that equal investment in both prevention and punishment is essential to curbing the troubling rise of economic crimes in the long run. Undoubtedly, this effort cannot be managed solely by the judicial system, police, or prosecution authorities; it requires the involvement of the entire society (Sadegh Nejad Nayini & Ebrahimi, 2015: p. 164).

The principle of transparency plays a crucial role in preventing economic crimes. Its primary function is to ensure free access to economic information, which helps build confidence among both domestic and foreign investors. Situational prevention of economic crimes relies on a fundamental model aimed at eliminating opportunities and conditions favorable for criminal activity. By making critical information publicly available, such as details regarding government tenders or the transfer of shares in state-owned companies, the likelihood of such crimes occurring can be significantly reduced. For example, when information about government contracts or the undervaluation of state assets is disclosed, it limits opportunities for corrupt practices, such as bribery in government tenders. Furthermore, transparency helps identify market obstacles for economic actors, enabling them to explore alternative choices. This pressure encourages governments to adjust their policies in order to attract more investment. Free access to economic information, as a vital aspect of transparency, is essential for enhancing a company's appeal to investors and serves as a key element in effective economic management systems (Sadegh Nejad Naini, 2024: pp. 68-69).

Article 5 of the Merida Convention, found in the second chapter concerning deterrent measures, policies, and methods against financial corruption, states that each member country, while respecting the fundamental principles of its legal system, must establish effective and coordinated policies to eradicate financial corruption. These common policies should empower society members in this area and reflect the principles of the rule of law, proper management of public affairs

and state property, as well as promoting financial integrity, transparency, and accountability to the law. The preventive measures outlined in this article aim to prevent financial corruption, and it is important to note that this article addresses not only financial corruption but also other banking and economic crimes.

The actions taken to enhance financial and banking transparency utilize various tools and resources that automatically and implicitly create a foundation for healthy business and commercial competition. This, in turn, contributes to the overall health of the economic system in society. Additionally, the principle of clarification will help address and resolve the questions and concerns that the public has regarding financial and banking issues.

4.2. Fighting Financial Crimes in Electronic Banking

After identifying the source of the crime, its turn is to profiteers and tax offenders. Financial crimes, as economic crimes, are criminalized, and punishment is also considered for this type of crime. Economic crimes have the potential to inflict irreversible harm on both the public and private sectors' economies.

Regarding international documents on financial crimes, we can refer to the Convention of the Organization of American States on the Prohibition of Corruption approved on March 29, 1996, the Convention on Combating Financial Corruption Committed by Officials of European Countries on May 26, 1997, and the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. Approved by the Organization for Economic Cooperation and Development on November 21, 1997. the Criminal Law Convention on Financial Corruption approved by the Committee of Ministers of the Council of Europe on November 4, 1999 and the African Union Convention on Preventing and Combating Financial Corruption approved by the Heads of State of the Union, approved on December 12, 2003.

All the above provisions indicate that financial crimes are criminalized and punishable. Because, on the one hand, the bank is a financial service provider and, on the other hand, it is known as an official institution, it acts as a communication bridge between the people and the central bank. If a bank is equipped with a smart banking system, banking activities will be carried out as soon as possible and with complete security. The quality of banking services has increased; transactions can be done at any time and place. Of course, because some countries, such as Russia and Iran, have economic sanctions, unfortunately these transactions are often not cross-border. Another important issue is to maintain the policy of protecting secrets and confidentiality in the banking system. Article 40 of the United Nations Convention to Combat Corruption mentions bank secrecy. The importance of this issue increases when there is an electronic banking system, but there is not enough knowledge about protecting the privacy of individuals in the cyberspace, or it is of little importance. In EFT financial and cyber banking crimes, the subject of violations of people's privacy and access to customer information has always been in the sights of hackers. Therefore, considering this importance, the electronic

banking system should protect the privacy and private information of people in the virtual space (related to banking systems) more than any other issue. Because cyberspace is a suitable environment for profiteers and financial criminals for crimes such as fraud, bribery, embezzlement, money laundering, and financial and tax frauds.

5. Conclusion

Today's world is unimaginable without digital technology. The growing development of virtual networks and the interweaving of different sciences with the Internet and digital technology is obvious. The spread of digital technology (especially artificial intelligence) is evident all over the world and in all jobs and fields, and the importance of learning computer science topics is not hidden from anyone. Economics, business communication sciences, and banking systems are also not immune from this. On the other hand, countries have no choice but to keep up with the digital world.

Nowadays, the world has become a global village due to the presence of communication tools in the virtual space. Therefore, one of the most important duties of governments is to educate and provide necessary and sufficient information to citizens in this field. Banking crimes have two aspects, public and private. The criminal, in a private aspect, harms the victim or a certain institution. In the general aspect of this crime, the criminal can paralyze the country's economy and make the economic cycle unhealthy.

Since the role of digital technology has recently become more prominent in the banking system, especially in developing countries, it is natural that many elderly people are not familiar enough with this mechanized and machine environment. On the other hand, teaching computer science is almost impossible for this age group of people. The financial and banking system is also tied to artificial intelligence, expanding rapidly and dynamically. Therefore, the lack of sufficient information and lack of familiarity with the elderly computer science completely attracts the attention of criminals for fraud extortion, etc. Providing bank cards, hacking Internet banking, sending money on the Internet to participate in the lottery, placing the second code of a bank card in another's possession, and other cases all indicate the abuse of the elderly by criminals due to their lack of knowledge.

The next important thing seems to be the weakness of monitoring banking systems by the central banking system. Digital technology and artificial intelligence act as a double-edged sword. Because it can also be placed in the way of serving humanity honestly. It can also inflict irreparable blows on a person for being on the wrong path. Converting traditional banking to electronic banking can be beneficial for members of society, but only as long as it does not deviate from the standards and norms established in society. This important thing will be implemented when there is special supervision of the banking systems. For example, when a hacker enters the victim's Internet banking page to hack his information by sending malware or a Trojan, the banking monitoring system must be powerful

and sensitive enough to track the case while protecting the information. The customer should report this crime as a cybercrime to judicial and legal authorities. Therefore, it is necessary to mention and mention cybercrimes in legal texts and texts along with their punishment, so that when a crime occurs, it can be referred to that legal article. Stating the guarantee of proper implementation by the legislator on the one hand and considering a punishment that has both a disciplinary aspect and a preventive aspect on the other hand is very necessary in preventing and punishing this crime.

Some government jobs play a very vital role in the safety and well-being of the public. Therefore, their safety should be guaranteed financially and physically by the government and the institutions in question. For example, the person who is responsible for the protection and guarding of the data center to maintain security or get rid of the problems of livelihood in case of emergency provides information to the criminals in various ways in exchange for a huge bribe. It can cause irreparable damage not only to the victim but also to the whole society. Therefore, providing the financial and life security of the supervisors of the banking system is one of the necessities of banking. Appropriate training related to the field of work, appointing experts according to the field and working conditions, and choosing qualified and qualified people in various fields of the banking system—all these things can be of great help in improving the level of security in banking transactions and activities.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Aghababaei, H. (2007). New Criminal Policy Strategies in the Fight against Corruption with an Emphasis on the Crimes of Bribery and Embezzlement. *Mofid Ghom Legal Quarterly, No. 1,* 119-136.

Akbaş, F. (2023). Bankacılıkta Dijital Dönüşüm ve FinTech. *Uluslararası Ekonomik Araştırmalar Dergisi, No. 9,* 1-12.

Alhajeri, R., & Alhashem, A. (2023). Using Artificial Intelligence to Combat Money Laundering. *Intelligent Information Management, No. 15,* 284-305. https://doi.org/10.4236/iim.2023.154014

Azizi, A. (2020). The Role of Bank Managers in Preventing Economic Corruption in the Islamic Banking System. In *Islamic Jurisprudence and Law Research Conference* (pp. 1-20). Qanun Yar Institute.

Carson, B. (2024). *What Is Blockchain*? (pp. 1-7). McKinsey & Company. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain

Ceylan, F. (2024). A Review of Central Bank Digital Currency: Current Status and Changing Trends. *İzmir İktisat Dergisi, No. 39,* 568-589. https://doi.org/10.24988/ije.1422562

Charles, M. (2013). *Electronic Banking in Uganda: The Modes, Risks and the Legal Challenges of Electronic Banking* (pp. 1-51). Kampala International University College of Law.

Coşkun, N. (2004). Karaparanın Aklanması Suçu. *Selçuk Üniversitesi Hukuk Fakültesi*

Dergisi, No. 12, 229-261.

Demir, O., & Odabaşi, H. (2022). Merkez bankasi dijital para sisteminin avantaj ve dezavantajlari neler olabilir? *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, No. 61,* 199-222. https://doi.org/10.18070/erciyesiibd.981733

Digamberrao Gudup, S. (2016). The Study of Frauds and Safety in E-Banking. *Anveshana's International Journal of Research in Regional Studies, Law, Social Sciences, Journalism and Management Practices, No. 8,* 213-216.

Farkhondeh, E. et al. (2023). Analysis of Legal Works and Concepts of Money Laundering. *Law Studies Quarterly, No. 31,* 475-504.

Forati, M. (2019). *The Role of Banks in Economic Crimes* (pp. 66-82). Bar Association.

Ghorchi Beigi, M. (2018). A Qualitative Analysis of White Collar Crime: Understanding Contexts and Motives. *Social Issues of Iran, No. 10,* 217-238.

Hemmati, P. (2011). Security Policies and Tools in Electronic Banking. In *6th Conference on Economics and Electronic Commerce* (p. 3). https://iuea.ir/files/site1/pages/document/file13950204/abzarhayeamniatidarbankdarie-lectronic13950208.pdf

Hosseini, H., & Azari Matin, A. (2016). Prevention of Money Laundering Crime in the Monetary and Banking System. *Criminal Doctrines of Razavi University of Islamic Sciences, No. 10,* 135-154.

Jakubiec, W., & Kuliński, M. (2023). The Phenomenon of Economic Crime: Threats and Contemporary Trends. *Scientific Journal of Bielsko-Biala School of Finance and Law, No. 27,* 55-58.

Kato, C. I. (2019). Legal Framework Challenges to E-Banking in Tanzania. *PSU Research Review, No. 3,* 101-110. https://doi.org/10.1108/prr-06-2018-0016

Korkmaz, F. (2020). Dolandiricilik suçunun bilişim sistemlerinin araç olarak kullanilmasi suretiyle işlenmesi. *Ankara Üniversitesi Hukuk Fakültesi Dergisi, No. 69,* 1415-1436. https://doi.org/10.33629/auhfd.848992

Mirsaeidi, M., & Zamani, M. (2013). Economic Crime, Definition or Code? *Criminal Law Research, No. 2,* 167-199.

Mohaddes Khalasi, M. R. (2016). Evaluation of the Effect of Electronic Banking on the Performance of the Interest-Free Banking System. In *Management and Entrepreneurship Conference* (pp. 1-24).

Moradi Ghale, S. (2013). Money Laundering through Digital Currencies. *Legal Research, No. 5,* 271-290.

Mustafa Ali, A., & Edris Mohammed, R. (2023). Money Laundering in the Digital Age: A Comparative Analysis of Electronic Means in Egypt, Jordan, the UAE and Iraq. *Pakistan Journal of Criminology, No. 15,* 193-212.

Najafi Tawana, A., & Karimi, F. (2021). Policy to Prevent and Fight the Crime of Internet Fraud. *Ghaun Yar International Quarterly, No. 16,* 419-446.

Nasiri, S. (2016). Money Laundering and Ways to Deal with It. *International Accounting and Management Conference, No. 4,* 1-32.

Qashqai, Z. (2022). Types and Effects of Risk in Electronic Banking. *International and National Conference on Accounting Management Studies and International Law, No. 6,* 1051-1035.

Rashid, O. et al. (2021). The Impact of Electronic Crimes on the Risks of Banking Financial Services in Light of the Increasing Use of Banking Information Technology and Communications. *Academy of Entrepreneurship Journal, No. 27,* 1-10.

Riemer, S. H. (1942). Embezzlement: Pathological Basis. *Journal of Criminal Law and*

Criminology, No. 5, 410-423.

Sadegh Nejad Naini, M. (2024). The Role of Transparency in the Prevention of Economic Crimes. *Encyclopedia of Economic Laws, No. 31,* 57-79.

Sadegh Nejad Naini, M., & Ebrahimi, Sh. (2015). Criminal Analysis of Economic Crimes. *Criminal Law Research, No. 5,* 147-174.

Sultan Altaie, Y. H., & Tayyeh Mohammed, S. (2020). The Role of Digital Banking Services in Enhancing Customer Trust. *PalArch's Journal of Archaeology of Egypt/Egyptology, No. 17,* 12397-12412.

Valvi, E. (2023). The Role of Legal Professionals in the European and International Legal and Regulatory Framework against Money Laundering. *Journal of Money Laundering Control, No. 26,* 28-52. https://doi.org/10.1108/jmlc-12-2021-0139

Yang, Y. (1997). *The Security of Electronic Banking* (pp. 1-12).

Yildiz, Ü., Kabakçi Günay, E., Günsoy, G., & Günsoy, B. (2022). Socioeconomic Determinants of Economic Crimes in Turkey: Dynamic Panel Data Analysis. *Yönetim ve Ekonomi Araştırmaları Dergisi, No. 20,* 253-275. https://doi.org/10.11611/yead.1106685

https://www.banknet.gov/

https://www.dotin.ir