Iulia Brici

Babes-Bolyai University of Cluj-Napoca Department of Finance, Faculty of Economics and Business Administration, Romania E-mail: iulia.brici@econ.ubbcluj.ro

NEW TENDENCY OF ECONOMIC AND FINANCIAL CRIME IN THE CONTEXT OF DIGITAL AGE. A LITERATURE REVIEW

Review paper

UDK: 343.53:004.056:007

JEL classification: O2, O32, O38, H11, H26

DOI: 10.17818/DIEM/2022/1.13 Accepted for publishing: July 8, 2021

Abstract

This paper wraps together two big concepts. First of them is the economic and financial crime and the second one is the digitalization. Each one of them has its own sub-components. The economic and financial crime can be split in: corruption, shadow economy, money laundering or cybercrime. Also, the digitalization can be explained as being related to smaller components, such as: connectivity, use of internet or digital public services. We tried to identify the relationship between these two concepts. As time goes on, we notice that the classical methods of economic and financial crime are at the same level as they were in the past, but digitalization is increasingly making itself comfortable in the field, which is why these types of crime methods are blooming. The subject provides a long-term research because of the technological development. This literature review study paves the way for more extensive research in the form of an empirical research, in order to statistically identify which phenomenon affects the other and how it is actually happening.

Keywords: money laundering, cybercrime, fraud

1. INTRODUCTION

Being a topic of current interest, economic and financial crime provides a new research horizon. In the last years, this topic has been approached by many authors receiving a lot of definitions, and there were also identified a significant number of its destructive effects. These can be found at the economic and financial level, but also at the social and political level. The concept is a complex one and all its negative effects are highlighted by breaking the main phenomenon of economic and financial crime into components. These parts represent its most common forms, namely: corruption, shadow economy and money laundering.

As the technology progresses, these events are taking place, more often, in the online space. In order to approach and cover the gap in the literature, the topic refers to the relationship between the phenomenon of digitalization and economic and financial crime. The main objective is to synthesize the literature that has already been written on the subject and to describe the types of events that may happen at the intersection of digitalization with economic and financial crime. These two phenomena have been approached separately, but no studies have been conducted to

cover both of them and, of course, no author tried yet to capture the impact of technological progress on the components of economic and financial crime.

This impact can be seen from two different perspectives, which is why the research has to focus on highlighting the advantages and disadvantages of digitalization in this context. On the one hand, digitalization can be a beneficial process and has the role to help identifing attempts of fraud, corruption or other events that can affect the economy. This perspective is a positive one because it can help maintain a clean economic environment. On the other hand, digitalization can produce, through the various existing gadgets, ways to realize scams in the economic and financial field. Thus, I consider that the chosen topic is one of general interest and deserves to be developed.

The sources that have been used are based on scientific articles published in specialized journals, specialized books or other documents from national or international databases.

Section 2 of this article contains the theoretical approaches of the two concepts used during the study. Firstly, it was explained the notion of economic and financial crime and then each of its three subcomponents. Associated with each of these notions there is a specific indicator of quantification. Secondly, the other main concept was approached, the digitization, being also split into subcomponents and measurement methods.

Section 3 includes a review of the existing literature related to the topic, and section 4 represents the conclusions of the study. Following the writing of this article, we came to the conclusion that the subject was not approached deeply enough and the link between digitalization and economic and financial crime was not explained and statistically justified.

2. THEORETICAL APPROACHES

2.1. Economic and financial crime – concept

The concept of economic crime emerged in the twentieth century, the first scientists who provided this notion in their writings were Bonger (1905 and 1916) and Sutherland (1940). In the book *Criminality and economic conditions*, Bonger introduces the notion of "economic crime" as a result of a difference between it and street crime. His work refers to the crimes committed by traders and entrepreneurs on property. Also, in the book *White-collar criminality*, Sutherland discusses the notion of "white-collar crime" by demonstrating the existence of a high-class crime, which is punished by the criminal law. The study of these authors begins to grow and spread worldwide only at the end of the twentieth century, the beginning of the twenty-first century.

Sutherland's study proved to be partly true, because economic and social development has created other categories of economic criminals who are not necessarily from the upper classes. A study conducted by Letia (2014) on a group of 69 countries investigated approximately 350 cases of economic crimes. Following this, the profile of the business criminal looks as it follows: man between 36-45 years old, employed in the financial field, commits frauds against the employer; or has a management position in the company where he has been working for over 10 years and commits crimes to achieve a leadership position, taking advantage of the weakness of the control structure.

In a study made by Queloz (2002), the author defines economic crimes, by comparison with organized crimes, as an abuse of good faith in business relations and which undermine the credibility and security of the economic and financial order. Thus, it cause not only financial, but also economic and social damages.

Thus, crime can be approached from several perspectives. According to Moldoveanu (1999), from a legal point of view, it is the set of human behaviors considered crimes and sanctioned according to their nature, within a criminal law system. In another study, Achim and

Borlea (2019) cited Niţă (2008) who views crime from a social point of view as a mass social phenomenon that manifests regularly and can never be stopped from its roots.

Also, in 2019, Achim and Borlea stated that, at international level, there is no common definition, regarding the economic and financial crime, but the concept can be associated to numerous notions such as: corruption, theft, cheating, embezzlement, data distortion, fraud, forgery, counterfeiting, data and document cover up or destruction, money laundering, tax evasion, crimes regarding accounting books or faked offers.

According to Pantea (2010) crime can be viewed both at a microeconomic and at a macroeconomic level. The macroeconomic part refers to crimes that attack national or even international security. People who commit such crimes are well prepared, so their facts can cause harm at national or international level, such as fraud at a higher level or customs offenses with cross-border effects. The microeconomic part refers to the crimes committed by violating at the minimum level the social values, producing minor damages and endangering the state or its citizens.

The reason why a unitary definition of this concept could not be established is the continuous evolution of the ways in which such fraudulent activities can be executed. In order to identify the definitions given by various authors to the notion of economic and financial crime, I have created Table 1.

Table 1 Definitions of economic and financial crime

Year	Author	Definition
2010	Romanian Academy	"all criminal acts for a given period"
2010	Pantea	"the crimes provided by the special laws with dispositions belonging to the business criminal law, refers to the competition, commercial societies intellectual property, money laundering, banking regime, securities, tax evasion, accountancy regime, customs procedure, public authority, lands etc."
2014	Leţia	"all those forms of non-violent crime causing a financial loss", "abuse of trust, speculating on the good faith of participants in economic life, credibility and apparent stability of the financial, commercial, banking, documents"
2016	Aniței, Lazăr	"all illegal acts and deeds committed by individuals, associations, companies or organizations, in connection with the conduct of business or financial, banking, customs, commercial transactions, through the use of fraud, fraud, breach of trust, forgery of turnover, money laundering, fraudulent bankruptcy, tax evasion, insurance policies"
2016	Pricewaterhouse Coopers	"asset missapropriation, bribery and corruption, accounting and tax fraud, cybercrime, procurement fraud" and "it represents a persistent threat to business and business process"
2020	US legal definition	"the illegal acts committed by an individual or a group of individuals to obtain a financial or professional advantage. In such crimes, the offender's principal reason is economic gain. Cyber crimes, tax evasion, robbery, selling of controlled substances and abuses of economic aid are all examples of economic crimes."
2020	Interpol	"financial crime ranges from basic theft or fraud committed by ill-intentioned individuals to large-scale operations masterminded by organized criminals with a foot on every continent. These are serious criminal activities whose importance should not be minimized as, over and beyond their social and economic impact, they are often closely linked to violent crime and even terrorism."

Source: Authors processing

Also, speaking of a certain classification, economic and financial crime encompasses several forms. According to Achim and Borlea (2020) these forms are enumerated in Figure 1 below:



Source: Authors processing based on Achim and Borlea (2020)

Figure 1 Main forms of economic and financial crime

2.2. Economic and financial crime – main forms

As it was specified in the introduction of this paper, the main forms of economic and financial crime are: corruption, shodow economy and money laundering. The first one, corrpution, refers to the illegal use of the public resources for a personal gain, according to the World Bank. According to Achim and Borlea (2019), corruption can be classified into three categories: small, medium and big. The criteria of establishing in which category to put a certain corruption activity can be seen in Table 2.

Table 2 Criteria of establishing corruption category

I	The value of the bribe or other way used exceeds 10,000 euros.
II	The value of the damage caused exceeds 200,000 euros.
III	Regardless of the amount of the damage, the crime is committed by people with important positions for the country.

Source: Authors processing based on Achim and Borlea (2019)

Corruption can be measured by using the Corruption Perception Index, which aggregates data from different surveys on the perception of corruption registered in the public sector in different countries of the world. This index is established annually on a scale from 0 (very corrupt), to 100 (very clean), for a number of 180 countries, from 1995 until now.

The second form of economic and financial crime, the shadow economy, is another destructive activity. Among the similar notions used for this concept are: unofficial, unstructured, marginal, gray, illegal, hidden, secondary, occult economy or counter economy. All these secondary notions sum up the same definition, namely that the shadow economy includes all economic activities that have not been registered, but which, if are taken into account, would have contributed to a country's Gross Domestic Product (Schneider, 2015). Examples of shadow economy activities, we can mention: avoiding of paying taxes or contributions to social insurance, avoiding the requirements of meeting legal standards on the labor market, avoiding compliance with administrative procedures, generating legally prohibited goods.

Shadow economy can be measured using the database elaborated by Schneider (Medina and Schneider, 2015), in which the size of shadow economy is calculated as a percentage of the official GDP, for a number of 158 countries, starting from 1991.

The third main form of economic and financial crime is money laundering. According to OECD, it is the process of hiding illegally produced sources, through criminal proceedings, in order to give them a seemingly legal origin. Examples of such activities are the following: the transfer of goods derived from illegal activities in order to cover their origin, the hiding of the nature of the property of a good derived from committing an illegal activity, the acquisition of goods knowing that they are the object of an illegal activity.

Money laundering level can be quantified by using the Basel Anti-Money Laundering Index, which measures the risk of money laundering and terrorist financing in over 129 countries around the world. The Basel AML score is calculated starting from 2012.

Considering these main components of economic and financial crime and the measurement methods corresponding to each one of them, Achim and Borlea (2019) have developed a separate index, economic and financial crime index (CSL) built as an arithmetic average score of corruption, shadow economy and money laundering. The economic and financial crime score ranges between level 0, reflecting the lowest size of economic and financial crime and level 1, reflecting the highest size of economic and financial crime. CSL is used to quantify the level of economic and financial crime specific to a particular country. It also helps in making comparative analyzes between states.

Both at the level of each component, but also after the aggregation of the three components in a single index, there is an area division specific to each country. For example, following a study on 45 European countries for the period 2005-2020 by Achim et al. (2020) the highest impact can be found in the countries of Southern Europe, but also in Central and Eastern Europe. At the opposite pole are the Western countries, but especially the Northern countries. The causes of the areal division, are of economic, political or legal nature as economic growth rate, institutional quality, quality of regulation, fiscal pressure, but also of social and cultural nature such as culture, fiscal morality or religion.

2.3. Digitalization - concept

Digitalization is a phenomenon we are currently facing with. In a very simple definition, this involves transforming any information from analogical to digital. Digitalization is more than a conventional change. This can bring benefits or disadvantages. This process of transformation makes its appearance felt in many areas, changing mentalities and comes, consequently, with a process that requires a well-organized implementation plan. According to several writings, articles or interviews, there are many definitions that can describe digitalization. These are summarized in Table 3.

Table 3 Collection of digitalization definitions

Integration of digital technologies into everyday life by transforming traditional activities into digital ones.

The adoption of digital technologies in order to modify a business model with the aim of creating value from the use of new.

Digitalization means reorganizing the strategies and work methods of a company in order to obtain benefits with the help of new technologies.

Digitalization means improving communications and interaction in order to improve company's performance.

Digitalization means computerization of systems in order to have ease accessibility.

The use of digital converts classical information into digital, stores is easily, processes it quickly and share is very fast by using a network.

The digital world is made by processes of adopting digital technologies in individual, organizational or social contexts.

Digitalization transfers printed products to digital ones.

Digitalization is the management of business processes.

Source: Authors processing

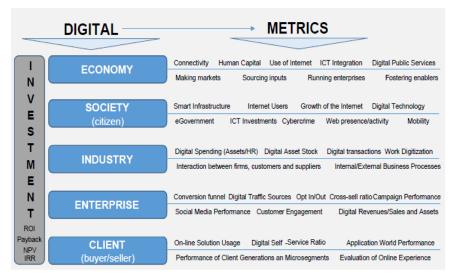
If we look at the microeconomic level, digitalization is about doing things in a way that helps in achieving the strategic objectives of a company. Firstly, it can facilitate innovation, which provides medium or long-term business continuity. Secondly, due to the digitalization, the sphere of clients or employees of a company can be positively influenced, the communication being more efficient. Also, due to digitalization, the company is positively influenced because the execution time can be shorter, which is why the results will come faster. At the same time, the risks can be minimized and the company will be less exposed. Electronic archiving can be a decision that attracts a higher degree of security. In this regard, high-performance systems are needed for ensuring safety and easy-to-perform processes. Even if a digital process replaces many of the classical activities, it must be chosen carefully because it is a thin line between security and exposure.

Dufva (2019) developed a study about understanding the future through the prism of the digital society according to which society has become more digitalized over time and most of the daily activities are performed using algorithms. The degree of digitalization, but also the repercussions that digitalization has, are difficult to perceive for many people. The authors introduce the term "digi-grasping" to analyze the level of constraint and involvement of society in the digital world. They believe that such an approach is necessary to shape this digitalized future.

Even if from many perspectives the digitalization process is put in a positive light, which brings progress, there are also opposite opinions, such as Weber (2019) who says in an article written for DeGruyter that for about 200 years ago, researchers are investigating the concern that technological progress can cause a decrease in the number of jobs. With the advent of the Internet, robots, self-driving machines and artificial intelligence, there is an increasing risk that many employees will be replaced by new technologies. Digitalization of an entire company would not only bring benefits. Absolute control over online activities can pave the way for cybercrime. Also, the ease of communication can have a negative impact on our social life. There is also a risk that these technologies sometimes fail and this can be fatal when we talk about fields like medicine.

2.4. Digitalization - measurement methods

Technological progress is a two-way street. Regarding the way of measuring digitalization, several studies have been made over the years and, their authors provides us a very useful set of indicators. Kotarba (2017) developed a study representing an analysis of indicators for measuring digitalization activities. Five main levels were analyzed, as follows: economy, society, industry, enterprise and client and we can see it in Picture 1 below.



Source: Kotarba, 2017

Figure 2 Digitalization dimensions and their primary metrics

The study is based on top public and commercial indicators used in the evaluation of the digital process. First indicator is Digital Density Index (DDI) developed by Oxford Economics and Accenture (Macchi, 2015). The purpose of DDI is to guide investments of business and public community in order to raise economic development. It contains 50 indicators, grouped into 4 activity areas. Metrics can take values between 0-100 reflecting the digital profile of each country. The second indicator is Digital Economy and Society Index (DESI) created by the European Comission in order to track the evolution of digital competitiveness in the EU member states. DESI is a composite index which contains five measuring areas: connectivity, human capital, use of internet, integration and digital public services. DDI and DESI reflect the high impact of competitiveness of country economies in the global context. DDI in oriented to economy, while DESI is including economic and social factors (eg. human capital potential).

Also, World Bank provides a well structured database, in The World Development Report 2016: Digital Dividends. This includes 183 countries. The set of indicators includes: Digital Adoption Index (DAI), DAI Business Sub-index, DAI People Sub-index, DAI Government Sub-index. The main index is the Digital Adoption Index, being used to measure countries' digital adoption across three levels of the economy, as follows: people, government and business. It takes values between 0 and 1, being the arithmetic mean of the 3 sub-indexes. Each of them includes the technologies necessary for development in the digital age. The original data available on-line were made in 2014, and those updated were made in 2016. DAI can help design a digital strategy to promote the adoption of technology by as many users as possible.

Chakravorti et al. (2017) developed a digitalization measurement index called the Digital Evolution Index (DEI) that includes data on 60 countries. Its purpose is to follow the evolution of the digital world. Following this study, there are certain areas where the changes from classic to digital occur faster.

Another way to measure digitalization is also provided by the World Bank. In the World Development Indicators set there is the High-technology exports indicator (calculated as a percentage of manufactured exports). Data are available for the period 2007-2018, for 264 states or groups of states.

The Global Competitiveness Index Historical Dataset from 2007 to 2017 provided by World Economic Forum, includes series such as: innovation and sophistication, technological adoption, mobile broadband subscriptions, individuals use of internet, FDI and technology transfer, firm-level technology absorption, availability of latest technologies and internet access in schools. These data are available for 159 states or groups of states and can be very useful in quantifying the degree of digitalization.

Taking into account the existing indicators for measuring the two variables, we can create a more comprehensive methodology in order to achieve the final proposed goal. This is a line of research that we will address in the future with great interest.

3. LITERATURE REVIEW

In the last years, a lot of researchers have identified interferences between the field of economics and the phenomenon of digitalization. This section makes possible a journey through the existing specialized literature and captures the gap that has to be covered.

A study made by Gaspareniene and Remeikiene (2015) claims that one of the most important problems we face is due to the activities realised in cyberspace. In this way, due to electronic transactions or made through social networks, even if the money circulate, most of these operations do not generate tax that goes to the state budget. Because of this, the phenomenon of digitalization receives another reason to be studied. The methods used in this research include comparative analyzes between existing articles in the literature. Digital shadow economy is the

new concept which is brought into discussion. It identifies forms and channels to make transactions on the black digital markets. This study innovated by highlighting the differences between the classical and digital economy.

Continuing this study, Gaspareniene et al. (2016) conducted an analysis on the attitude of consumers towards the digital shadow economy. The more transactions are made in the digital space, the more the number of illegal digital operators increases. For this reason, it is necessary to discourage participants in activities specific to the digital shadow economy. The results of this study showed that consumers distinguish criminal activities from illegal activities, punished according to their severity. Most people who took part in this survey believe that the digital shadow economy takes place in cyberspace, and thus they avoid paying taxes to the state budget online. The need to set up a department to prevent and penalize illegal activities in the digital space increases with the number of these negative events.

In order to fill the gap on the subject she addressed, Gaspareniene et al. (2017) returns with an article to establish a clearer definition of the concept of digital shadow economy and to identify its characteristics and ways of distribution. Due to this study, the literature has benefited from a definition that refers to illegal activities, such as the provision of digital services and online trade of goods, which violate legal regulations in order to obtain benefits for both the trader and the perosn who procured them. This definition highlights both the features of the phenomenon and the ways in which it distributes.

A study developed by Berdiev (2016) examines the relationship between financial development and shadow economy. The author used data from 161 countries, over the period 1960–2009. The methodology is represented by a panel vector autoregression model. The results showed that financial development is reducing the level of the shadow economy. There exists also some evidence of reverse causality between the variables. Thus, a shock to shadow economy obstructs financial development.

Another study made by Elgin (2013) examines whether the emergence and rapid spread of the internet has facilitated the shadow economy. The study is based on data from 152 countries for the period 1999-2007. The results of the study indicate that the association between the use of the internet and the level of shadow economy interacts with GDP per capita.

In a study conducted by Armey et al. (2014) there was put into discussion the hypothesis that electronic payments can reduce crime. The results of the study showed that there is a negative and statistically significant relationship between access to electronic payments and the incidence of events such as robbery or burglary. Also, electronic transactions does not have a big impact on reducing non-economic crimes such as homicide or rape. This article provides evidence that technology that allows the proliferation of transactions without the use of cash discourages crime.

In another study developed by Immordino et al. (2018) the authors claim that non-cash payments decrease the number of tax evasion cases. Using European data, they found evidence that debit or credit card payments are negatively linked to VAT evasion. Also, withdrawing cash at ATMs from electronic cards encourages VAT evasion.

In a study made by Ryman-Tubb et al. (2018) the authors try to identify how artificial intelligence can have an impact on payment card fraud identification. The benchmark shows that eight methods bring performance in the industry. The results also show that there is a gap in research that can help reducing payment card fraud.

A very suitable research article on our topic written by Achim et al. (2021) analyzed the impact of technology on economic and financial crime, using data for a group of 185 countries. The analyzed period was from 2012 to 2015. The authors found that on average, the size of economic and financial crime is double in the countries with low income, in comparison with the countries with high income. Their conclusion was that increasing the technology minimizes the level of economic and financial crime. In terms of control variables, like economic development, quality of

governance, tax burden, unemployment, press freedom or religion, also have influence on economic and financial crime. This study is original by conducting the analysis on subsamples in order to better detect the economic and financial crime related to the size of economic development.

If we refer strictly to the financial field, the information itself has been transformed. Database architectures can hide cybercrime algorithms. Cybercrime is not necessarily something to be afraid of, but a reality. New products and services may set a different pace than traditional ones. In this sense we mention, as an example in the financial field, the contactless cards, which are more and more used. These bring a lot of benefits that we all know. They are easy to use, they make payments much faster and, in the context of the pandemic, they also reduce the contact we would have to face through classical cash payments. However, the cards are not as secure as they seem. With the help of specialized card readers that criminals have, the data on the card can be copied instantly, without the cardholder having given his consent or without even realizing it. Of course, transactions without the need of the security PIN code are of small value and it do not represent a great benefit for the offender, but performed repeatedly may be the reason for continuing these criminal operations. The cardholder can reduce the loss by resetting off-line counters, so he can set transactions to one per day. The most recommended option is to lock the card and transfer the balance of the old card to a new one.

According to Scheau (2018) there are several methods of obtaining data from the card, fraudulently. The best known method is skimming. This involves obtaining data from the magnetic stripe of the card using a device mounted on an ATM / POS. After doing this, with the help of a computer program, the data of the respective card can be used or transferred to other people. Among the methods used at ATMs are: magnetic tape copiers, PIN code copiers, door skimmer and video camera, vandalism, cash trapping in ATMs or black boxes. With the help of the POS, which reads the information stored on the card, other skimming operations can be performed. Through POS skimmers, the information stored in the POS is transmitted directly to the server connected to the database. Many of these crimes go unnoticed and, unfortunately, unpunished.

Besides skimming, computer attack by vectors of infection is another well-known method of crime in the financial field. These vectors can be installed in e-mail accounts, in external media devices or in the internet browsers. Phishing is another method that allows computer crime in the financial field. This is an information security management issue.

In the context of these crimes, the legislation should be modified taking into account new existing technologies. Regarding the crime related to cards, there should be ways to encrypt the cards so that to be impossible to transfer the confidential data corresponding to it. A positive step in this regard was made because the authentication is no longer done by typing the PIN code. Now is done by fingerprint. As criminals move very fast, there will be ways to obtain a fingerprint, for example by simply sticking an adhesive tape on the authentication strip. Maybe a more efficient method would be facial identification or voice recognition, but the process of collecting the necessary resources would be long. For money laundering crimes, there should also be a legislative framework according to the ways in which these acts take place. It would also be welcome to make devices for identifying and preventing suspicious transactions. It would be ideal to have security programs that provide protection of confidential user data, but also easy recovery of data in case of loss.

Another method in which cybercrime can occur is represented by cryptocurrencies. One of the most important features of cryptocurrencies is their anonymity. Because of this, criminals in the field are encouraged to commit cybercrime.

Over time, a lot of scams have been made with the help of cryptocurrencies. Every year, several million internet users are affected by cyber attacks done through cryptocurrencies. Among them, Şcheau (2020) mentions Plexcoin, a cryptocurrency that capitalized 15 million US dollars. Administrators were caught and punished. Another case was Benebit, which through a well-organized marketing campaign involving images of influencers such as: Centratech, fighter Floyd Mayweather or singer DJ Khaled have raised 32 million US dollars by the time they were discovered.

Many crimes are committed through fake mobile applications. These are available in the phone-specific app store and are quite difficult to detect. Extremely many people fall prey to these crimes, because they seem to be harmless applications, but when we accept any requested permission, the application administrators can access our confidential data related to bank accounts. Usually, these phantom applications are recognized because there are some mistakes in their name or the representative image is of a well-known brand.

Most scams are sent by email. Even though at first sight it was difficult for us to identify them as crimes, now they are dangerous only for the elderly people or those who do not know how to use gadgets. They are vulnerable when they receive messages in which they are charged to send an amount of money to invest in a business or to claim an imaginary reward.

In 2019, crimes committed with cryptocurrencies amount was about 4.26 trillion US dollars. Among them, Şcheau (2020) recalls the exchange between BITPoint and a Japanese currency. Following this exchange, the damage was about 28 million US dollars. Among the electronic coins that were stolen are even the most well-known, namely: Bitcoin, XRP, Litecoin, Ethereum or Bitcoin Cash.

Also in 2019, there was a theft of 40 million US dollars through an exchange with Binance. Unfortunately, the attack was not stopped in time, the hackers being very skilled. Also in June 2019, 6 individuals stole 27 million US dollars from 4,000 victims in 12 different countries. The event had a very big impact. This type of attack is called "typosquatting" and involves fooling victims into gaining access to their wallets with cryptocurrencies.

In an article, Caporale et al. (2019) addressed the issue of non-linearities, cyber-attacks, and cryptocurrencies. The authors used a Markov-switching non-linear specification to analyze the effects of cyberattacks on cryptocurrencies. The analyzed period was 2015-2019. The results showed that there are important negative influences of cyber attacks on the volatility of cryptocurrencies.

We can conclude that cybercrime made with the help of cryptocurrencies are very common and dangerous. To avoid such events we must be careful not to invest in cryptocurrencies that we do not know. Usually, all fraudulent offers come by email or advertisements. It is necessary not to share confidential data about our cryptocurrency wallets with anyone.

Following the selection of existing literature, we could see that over time the authors have approached the issue of digitalization from various perspectives. Some of them, and perhaps even the most consistent part, have studied the influence of digitalization in the context of the fluctuations observed in the level of the shadow economy. In less cases, there have also been identified writings in which digitalization has collided with other components of economic and financial crime. This paper, following everything that has been written on this subject, aims to open a path of research that includes the entire phenomenon of economic and financial crime. By identifying indicators for measuring each phenomenon, a lot of statistical processings can be created in the future to see the connection between these two phenomena.

4. CONCLUSIONS

Our paper represents an overview of the existing information on the topic, but also a way to highlight the general interest for it and also the motivation for choosing to approach it.

Even if the literature in the chosen field is generous, there could not be identified articles written exactly about the interference between digitalization and economic and financial crime. The aim of the study is to cover up this gap in the literature by identifying measurement methods of these two phenomena.

The topic is a new one, of current interest, but which will continue to be interesting as technology advances. The study on this subject offers a long horizon of research. Digitalization will

be increasingly implemented in the economic and financial field, and the methods by which customers / users will be helped or harmed will increase, step by step.

As a future research idea in the continuation of this study, we propose approaching the subject from a methodological and statistical point of view and to deepen the methods of quantification of these two processes.

A very important aspect to approach in the future is the cryptocurrency market. It has also been described in the literature review section, in the light of recent events that have represented fraudulent activities, which truly identify the link between economic and financial crime and digitalization. Also, banking crimes deserve much more attention. For these branches, the subject allows further development due to the approach of banks' privacy policies, security measures, sanctioning policy among these types of crimes, but also in identifying more ingenious methods of identifying fraudulent acts.

Our future research in this field aims to help develop methods for controlling and measuring the phenomenon of economic and financial crime, in the context of digitalizing all sectors of activity in the financial-banking domain.

Acknowledgement

This work was supported by a grant of the Romanian Ministry of Education and Research, CNCS - UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174, within PNCDI III.

REFERENCES

Achim, M.V., Borlea, N.S. (2019), Criminalitatea economico-financiară. Corupție, economie subterană și spălarea banilor. Cauze, efecte, soluții. Abordări teoretice și practice (Economic and financial crime. Corruption, shadow economy and money launderng. Causes, effects and solutions. Theoretical and practical approach), Economica Publishing House, Bucharest; https://doi.org/10.1007/978-3-030-51780-9

Achim, M.V., Borlea, N.S., Văidean, V.L. (2021), Does technology matter for economic and financial crime? A panel data study, Technological and Economic Development of Economy, 27(1), 223-261; https://doi.org/10.3846/tede.2021.13977

Achim, M.V., Borlea, N.S. (2020), Economic and financial crime. Corruption, shadow economy and money laundering, Springer Nature Switzerland AG, doi:10.1007/978-3-030-51780-9. https://doi.org/10.1007/978-3-030-51780-9

Achim, M. V., Borlea, N.S., Miron, G.M., Brici, I. (2020), Economic and Financial Crime in Romania in the Context of European Countries, RSEP Conference Proceedings Book, Istanbul, pages 47-57; https://doi.org/10.1007/978-3-030-51780-9

Aniței, N.C., Lazăr, R.E. (2016), Evaziunea fiscală între legalitate și infracțiune, Universul Juridic Publishing House, Bucharest;

Armey, L.E., Lipow, J., Webb, N.J. (2014), The impact of electronic financial payments on crime, Information Economics and Policy, United States; https://doi.org/10.1016/j.infoecopol.2014.10.002

Berdiev, A.N., Saunoris, J.W. (2016), Financial development and the shadow economy: A panel VAR analysis, Economic Modelling; https://doi.org/10.1016/j.econmod.2016.03.028

Bonger, W. (1916), Criminality and economic conditions, Little, Brown, and Company, Boston;

Bucur, D. (2011), Criminalitatea transfrontalieră și economia globalizată, Pro Universitaria Publishing House, Bucharest; Caporale, G.M., Woo-young, K., Spagnolo, F., Spagnolo N. (2019), Non-Linearities Cyber Attacks and Cryptocurrencies, Finance Research Letters; https://doi.org/10.1016/j.frl.2019.09.012

Chakravorti, B., Bhalla, A., Chaturvedi, R.S. (2017), 60 Countries' Digital Competitiveness, Indexed, HBR;

Dufva, T., Dufva, M. (2019), Grasping the future of the digital society, Futures, Volume 107, pages 17-28; https://doi.org/10.1016/j.futures.2018.11.001

Elgin, C. (2013), Internet usage and the shadow economy: Evidence from panel data, Economic Systems; https://doi.org/10.1016/j.ecosys.2012.08.005

Gaspareniene, L., Remeikiene, R. (2015), Digital Shadow Economy: a Critical Review of the Literature, Mediterranean Journal of Social Sciences, Rome-Italy; https://doi.org/10.5901/mjss.2015.v6n6s5p402

Gaspareniene, L., Remeikiene, R., Navickas, V. (2016), The concept of digital shadow economy: consumer's attitude, Procedia Economics and Finance, Rome-Italy; https://doi.org/10.1016/S2212-5671(16)30292-1

Immordino, G., Russo, F.F. (2018), Cashless payments and tax evasion, European Journal of Political Economy, Napoli; https://doi.org/10.1016/j.ejpoleco.2017.11.001

Interpol (2020), Financial crime, https://www.interpol.int/Crimes/Financial-crime;

Kotarba, M. (2017), Measuring Digitalization - Key Metrics, Foundations of Management, Poland; https://doi.org/10.1515/fman-2017-0010

Leția, A.A. (2014), Investigarea criminalității în afaceri, Universul Juridic Publishing House, Bucharest;

Moldoveanu, N. (1999), Criminalitatea economico-financiară, Global Print Publishing House, Bucharest;

Niță, N. (2008), Descoperirea și combaterea infracționalității economico-financiare, Tehnopress Publishing House, Bucharest;

Pantea, C. M. (2010), Investigarea criminalității economico-financiare, ProUniversitaria Publishing House, Bucharest; PricewaterhouseCoopers (2016), Global Economic Crime Survey, 2016;

Queloz, N. (2002), Criminalité économique et criminalité organisée, L'Économie politique, 2002/3 (no 15), pages 58-67; https://doi.org/10.3917/leco.015.0058

Remeikiene, R., Gaspareniene, L., Schneider, G. (2017), The definition of digital shadow economy; https://doi.org/10.3846/20294913.2016.1266530

Romanian Academy, lorgu lordan Institute of Linguistics (2010), Mic dicţionar academic, ediţia a Il-a, Univers Enciclopedic Publishing House, Bucharest;

Ryman-Tubb, N.F., Krause, P., Garn, W. (2018), How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark, Engineering Applications of Artificial Intelligence; https://doi.org/10.1016/j.engappai.2018.07.008

Schneider, F. (2015), Size and Development of the Shadow Economy of 31 European and 5 other OECD Countries from 2003 to 2015: Different Developments;

Schneider, F., Medina, L. (2015), Shadow Economies around the World: New Results for 158 Countries over 1991-2015, Cesifo Working Paper No. 6430, Category 1: Public Finance;

Sutherland, E.H.~(1940), White-collar~criminality, Holt, Rinehart~&~Winston, New~York; https://doi.org/10.2307/2083937.

Şcheau, M.C. (2018), Criminalitatea informatică privind transferurile financiare, Economic Publishing House, Bucharest; Şcheau, M.C., Crăciunescu, S.L., Brici, I., Achim, M.V. (2020), A cryptocurrency spectrum short analysis, Journal of Risk and Financial Management; https://doi.org/10.3390/jrfm13080184

USLegal (2020), Economic Crime Law and Legal Definition, available on-line at: https://definitions.uslegal.com/e/economic-crime/;

Weber, E., Bellmann, L., Moller, J. (2019), Special Issue: Digitalisation and the Labor Market; https://doi.org/10.1515/jbnst-2019-0031

World Bank (1997), Helping Countries Combat Corruption: The Role of the World Bank, The World Bank Development Research, Washington DC;

World Bank (2016), World Development Report 2016: Digital Dividends, available on-line at: https://www.worldbank.org/en/publication/wdr2016, accessed on 28th of October 2019;

World Bank (2019), High-technology exports, available on-line at: https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS, accessed on 20th of January 2020;

World Economic Forum, Global Competitiveness Index Database 2007-2017, available on-line at: http://www3.weforum.org/docs/GCR2017-2018/GCI_Dataset_2007-2017.xlsx, accessed on 28th of October 2019.