ARMG Publishing "Thinking ahead"

Business Ethics and Leadership, Volume 5, Issue 3, 2021
ISSN (online) – 2520-6311; ISSN (print) – 2520-6761

Banks' Digital Challenges

http://doi.org/10.21272/bel.5(3).87-96.2021

Elena Stavrova, ORCID**:** https://orcid.org/0000-0003-0162-7916

PhD, Associate Professor, D. Sc., Finance, SWU "Neofit Rilski" – Blagoevgrad, Bulgaria

Abstract

Digital currencies make transfers in digital markets, providing transaction participants with many advantages: easy access to markets, maintaining the identity of participants in transfer transactions, even their application is constantly expanding when buying new and innovative goods. Banks are an integral and significant part of this turnover, which gives them additional advantages and direct effects and exposes them to additional difficulties and dangers. The increased interest in them was noted mainly due to the continuous growth of their market rate and the additional growth of cryptocurrency extraction. Most transactions with them are based on the regulations of the applicable law. Still, the possibility of being the object of a crime has provoked a backlash from financial supervisors to protect the rights of other market participants and especially banks as the most accessible of all. Although it is a legal system in place to prevent banking institutions from being involved in money laundering operations, digital currencies are now a new opportunity with the specific advantages that ensure their smooth transfer to the network. The leading business companies such as TESLA have offered the opportunity to buy electric cars with digital currencies, with the growing demand for cryptocurrency services. Partly aided by the rising value of essential natural resources, important components for building information infrastructure, and the Covid-19 pandemic, significant financial institutions have permanently established themselves in digital markets such as JPMorgan, BNY Mellon, and Morgan Stanley, BlackRock and many others. Despite the targeted actions of state regulatory institutions, whose duty is to ensure the public good "cybersecurity", the mass entry into these markets leaves consumers relatively unprotected. Money laundering or terrorist financing often provokes crises among regulatory institutions because they are usually accompanied by arms deals, drug trafficking, tax evasion, and others, as well as tax fraud, terrorism, and drug trafficking. A current application of digital currencies is their use to pay for services related to cyber attacks on financial institutions, objects of national security, etc. when the entire population suffers the damage. The new roles of financial institutions in the digital markets strengthen the notion of compliance as possible risk threats, realizing through compliance functions to automate and implement the integrated approach to all types of risk that accompanies the movement of digital financial assets. For some banking intermediaries, this has changed their cybersecurity strategy.

Keywords: Anti-Money Laundering, Digital Markets, Crypto Currencies, Blockchain, Compliance Functions.

JEL Classification: E42, E58, L51.

Cite as: Stavrova, E. (2021). Banks' Digital Challenges. *Business Ethics and Leadership*, *5*(3), 87-96. http://doi.org/10.21272/bel.5(3).87-96.2021.

Received: 04 June 2021 **Accepted**: 10 August 2021 **Published**: 13 September 2021

Introduction

In the crisis conditions, no matter what it is - financial, economic, or humanitarian as the crisis COVID-19, the appetite for taking additional risk by any institutions, regardless of their role and goals of participation in the financial markets, increase enormously. The development of the banking business digital environment has proven to be a partial solution and a replacement strategy for providing many financial services by financial intermediaries of various types and financial markets. This digital transformation process has directly impacted the relationships with their clients and the behavior of the different client groups for urgent adaptation to the new communication channels. These processes caused changes in the methods used in criminal or moral action by both financial intermediaries and their clients.

Despite the measures taken to minimize the occurrence and consequences of fraud in an organization by the government, companies, and professional organizations, fraudulent activities still occur, leading to high costs for society. The costs of establishing a legal framework, setting up regulatory and supervisory bodies to monitor the implementation of legislation, and follow-up are significant accounts in the budgets of central

banks and other types of financial intermediaries. According to Rhoda Weeks-Brown (2019) of the International Monetary Fund[1], that money laundering amounts to between 2 and 5% of global GDP per year, or in financial terms from 1.6 to 4 trillion US dollars annually. They are in an identical position Lyeonov, S.V., Kuzmenko O.V., Mynenko, S.V., Kwilinski, A.S., Lyulyov, O.V. (2020)[2], Tommaso, F.D. (2020)[3].

Given that this amount is proportional to the sum of global financial flows, we cannot fail to note the serious negative socio-economic consequences of this process for the global economy. For this reason, global and local government regulators are drafting regulations to minimize these effects and prevent these legalization operations. It is no coincidence that the participants in Global Government Forum (2021)[4] have found that the challenges of distance partnership have stimulated significant changes in communication channels and information arrays by moving to artificial intelligence methodologies to monitor transactions through a platform for accelerated knowledge sharing at levels of detail that did not exist in -early. Unquestionably, the considerable growth of the cryptocurrency market such as Bitcoin, Ethereum, Dogecoin, according to the world news agency CoinGecko[5] in the second half of August 2021, which monitored the market positions of 8884 cryptocurrencies registered a record level of the market capitalization of 2,108,486,906,329 dollars.

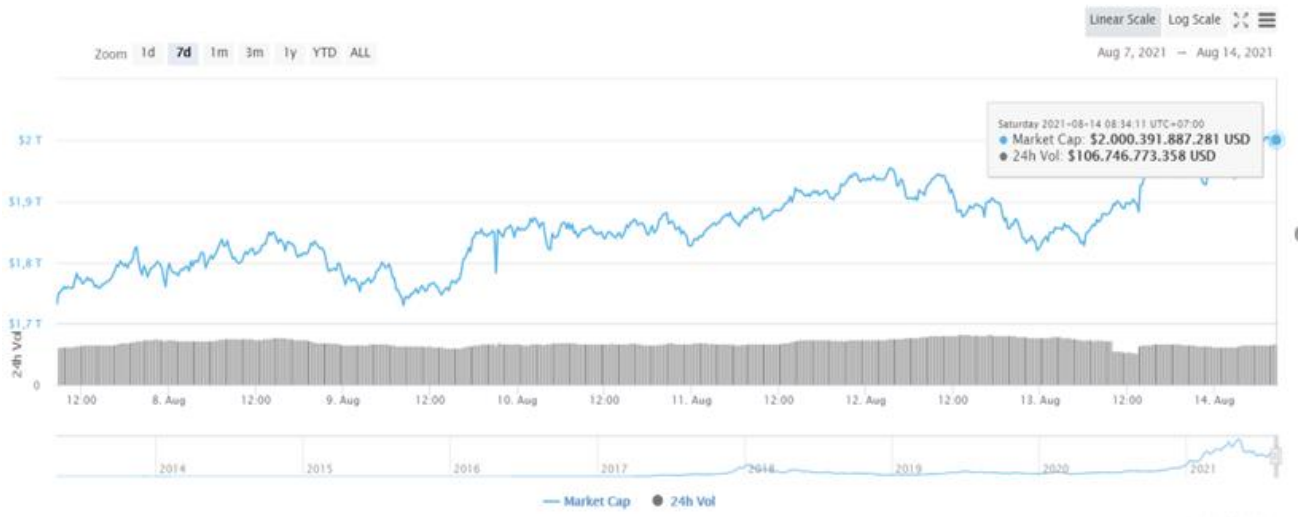

Figure 1. The Crypto Currency Market Capitalization

Source: https://news.coincu.com

With this impressive size, it is inevitably included in the field of observation and is accordingly positioned as a high-risk segment for transactions with this type of asset. Although, as they claim Andrii O. Zolkover and Marin Georgiev (2021)[6], N. Nenovsky and P. Chobanov (2021)[7], Vasilyeva, T., Sysoyeva, L., & Vysochyna, A.(2018)[8], if they are excluded from the government and banking financial systems and almost impossible to account for and forecast, they are capable of upsetting the balance in the monetary policy of the central bank and the macroeconomic policy of the government. Banking intermediation based exclusively on fiat, ie centralized money issued by a central bank, is also threatened by the migration of significant financial resources to decentralized funds, which are already subject to new market entrants FinTech and Bigtech, to the activity of which the main regulatory bodies − central banks have limited opportunities for control and regulation.

[1] Rhoda Weeks-Brown (2019). Cleaning Up. Countries are advancing efforts to stop criminals from laundering their trillions. Available at: [Link]
[2] Lyeonov, S.V., Kuzmenko, O.V., Mynenko, S.V., Kwilinski, A.S., Lyulyov, O.V. (2020). Determining the Rating of Ukrainian Banks on the Risk of Legalization of Illegally Obtained Income // Механізм регулювання економіки. 2020. № 3. 31-45. [CrossRef]
[3] Tommaso, F.D. (2020). The New Italian Legislation on Corporate Governance and Business Crisis. The Impact of Covid – 19 on SMEs and the Recent Rules to Mitigate the Effects. *Financial Markets, Institutions and Risks*, *4*(4), 91-108. [CrossRef]
[4] GGF (2021). Financial crime: five key trends from 2020 and how they played out. Partner Content on 22/02/2021
[5] Coincu News Available at: [Link]
[6] Zolkover, A.O., and Georgiev, Marin (2020). Shadow Investment Activity as a Factor of Macroeconomic Instability. *Financial Markets, Institutions and Risks*, *4*(4). Available at: [Link]
[7] Nenovsky, N., Chobanov, P. (2021). Digital currency Vs the crypto. Bloomberg Businessweek bg. July 2021, 44-53.
[8] Vasilyeva, T., Sysoyeva, L., & Vysochyna, A. (2016). Formalization of factors that are affecting stability of Ukraine banking system. *Risk governance & control: financial markets & institutions*, *6(4)*, 7-11. [CrossRef]

Business Ethics and Leadership, Volume 5, Issue 3, 2021
ISSN (online) – 2520-6311; ISSN (print) – 2520-6761

There is still a lot of research here that puts digital challenges facing banking institutions in the spotlight of the investor audience. Fr. Hayek (1976)[9] sees banks as part of a system that can issue their decentralized currencies, which replace fiats. Its currency pluralism provides a solution for businesses with difficulty accessing financial resources when governments cannot manage a centralized banking system. While introducing the term "denationalization of money", it gave a new opportunity to banks to directly stimulate the economy through their leadership position in the redistribution of free resources.

A review of the exchange rates of the main supranational currencies and the major digital currencies leaves no doubt that while decree money has relatively stable exchange rates, the same cannot be said for decentralized currencies. This high volatility makes this market for those looking for quick effects and thus directly affects their market rates. In Figure 2, the dynamics of one of the leading digital currencies can be seen. The transfer of resources from centralized to decentralized financial assets threatens the stability of the system due to limiting the main resource fund with which the state and the central bank can influence the implementation of the main functions of the financial system - to be its circulatory system, to transfer resources where important government commitments and policies are implemented − social policy, government debt management policy, etc.

Limitations of the Study

Due to the overview nature of this article, we cover only a limited aspect of commercial banks' activities, namely their participation in cryptocurrency markets and the threats that may follow from this process. In this article, we do not analyze trading in a particular cryptocurrency, despite their specific characteristics as such cryptocurrencies, whether they have specific characteristics when compared to fiat, maternity money. Here we stand aside from the high-tech debate over the clear and most widely mined cryptocurrency, bitcoin. Instead, we focus our efforts on presenting the dangers that all cryptocurrencies pose to banks as common and typical, based on the principled processes of money laundering. Our research focuses on the misuse of cryptocurrencies, which in themselves have a potentially massive impact on society and, due to their specific nature, generate an ethical interest, an issue when it comes to illegal actions. By limiting our investigation to the immediate impact of "obtaining the legal origin of digital assets" given the nature of the financial transactions with them, it is this financial aspect that is specifically addressed.

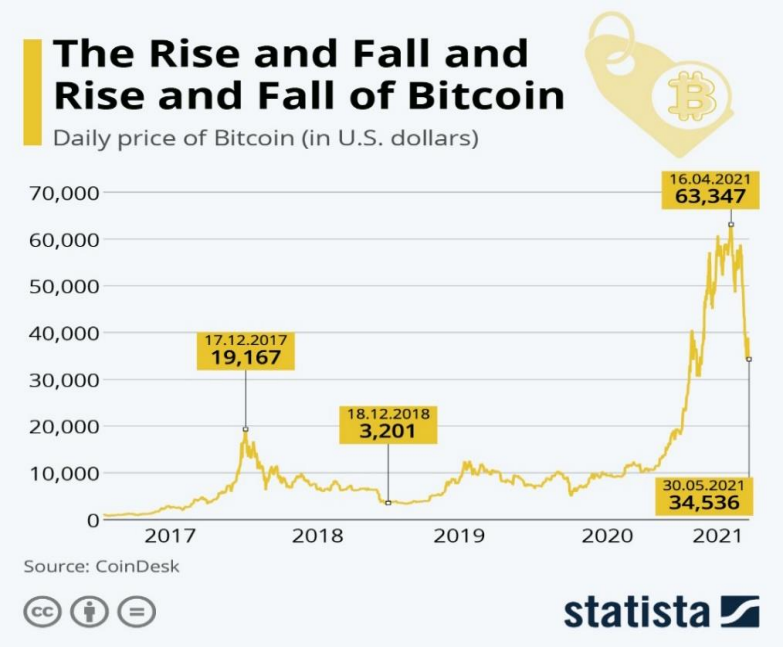

Figure 2. The Bitcoin Volatility 2017-2021

Source: www.CoinDesk.org

Methodology and Research Methods

This study, which focuses on the current risks in the financial markets associated with the emergence of digital, decentralized money, is epistemological in nature. The possibilities of using these relatively new types of

[9] Hayek, Fr. (1976). *The Denationalization of Money*, London: Institute of Economic Affairs.

digital financial assets, such as cryptocurrencies, to give legal origin to funds from a criminal or illegal source based on an ecosystem and further developed in the context of their manifestation in a dynamic and structural environment are explored. To achieve in-depth analysis, we have developed a research methodology. It will allow the phenomenon of digital challenges to banks to be presented as a general case and seek a projection of the digitalization impact on their use for legalization of illegal funds. It gives for the formation of two areas of intervention - theoretical and applied area. The study of the theoretical aspects regarding the money circulation in the legalization of resources of the illegal origin or tax-free.

In this context, analysis and synthesis will be applied. Through analysis, the framework for the regulation of the banking system will be examined to prevent these processes. Through synthesis, the accumulated information array will be summarized and presented appropriately. A sufficient number of literature sources have been summarized, based on which findings and recommendations for formulating the position of the author of this study have been formulated.

Main Theoretical Category

As early as 1976, the prominent Austrian economist and Nobel laureate in economics Friedrich Hayek spoke about the so-called "Good money" as a possible government solution to inflation, economic cycles, and the abolition of the state monopoly on the issuance of money. This idea was fully realized with the emergence of digital currencies and blockchain systems traded with them. Since the central banks do not monitor the issued cryptocurrencies, the aspiration of each criminal group is its financial resources to pass through a reputable financial institution with a significant customer base. For this reason, some of the world's largest operating banks, such as HSBC, Deutsche Bank, Danske Bank, and others, are involved in money laundering operations.

One of the most common scams in the financial industry is financial intermediaries to legalize cash flows from illegal or illegal business. The next stage in developing the supervision and regulation of cross-border cash flows is monitoring to prevent the use of these resources to finance terrorist regimes, terrorist groups and the inclusion of resources of such origin in international money exchange. This process has an accelerating effect due to the inclusion of banks in correspondent networks, which makes access to customer accounts possible in different jurisdictions. Although this type of mediation is extremely effective and widely used in global value chains, quite often the lack of a direct link between respondents in a transaction, which in turn limits the ability to verify the legal source of the funds involved. A similar case turned out to be that of Danske Bank, a Danish bank positioned in Estonia with a modest amount of equity, through which more than $ 200 billion was transferred to accounts in Deutsche Bank, JPMorgan and Bank of America. In 2020, the prosecutor's office in Frankfurt, Germany, fined Deutsche Bank AG EUR 13.5 million (US $ 16 million) for established violations related to criminal money as a result of transfers from Danske Bank A/S. The bank failed to notify supervisors of more than 500 suspicious financial transfers. During the period 2007-2015, these banks have consistently limited their receipts from Estonian bank accounts, but this has led to regulatory intervention, Regulatory fines, reputational damage, loss of business through risk reduction and loss of customer confidence, negative articles in the media about the bank's activities, additional restrictions in the operations carried out, the collapse of the stock exchange rates of the bank's securities, etc.

The international financial community has consistently expressed additional concerns about the potential of using cryptocurrencies to legalize proceeds of crime, make them legitimate or use them to finance terrorist acts. The most important international institution setting global standards and coordinating anti-money laundering policies is the Financial Action Task Force, whose documents have been adopted by more than 200 countries and jurisdictions from all continents (FATF, 2020)[10]. The main goal of this institution is to synchronize the actions and policies of countries to identify threats to their financial systems, to develop smooth rules against the ever-updating range of crimes against these systems, to organize the efforts of the international community to develop guarantees for preserving and preserving the "Integrity of the International Financial System" FATF (2012)[11]. This intergovernmental body prefers to apply a risk management approach (RBA), based on the identification, analysis, and assessment of the risks of money laundering and updating with the addition of a new area − "terrorist financing" (2018)[12]. The risk management approach aims to "ensure that measures to prevent or mitigate forms of financial crime" are comparable to the risks identified during the procedure. Cooperation with the institution enables the affected countries to flexibly and effectively

[10] FATF (2020). Financial Action Task Force − Annual Report 2019-2020, FATF/OECD, Paris. Available at: [Link]
[11] European Union. News. Available at: [Link]
[12] FATF (2018). Guidance for a Risk-Based Approach for the Securities Sector, FATF, Paris. Available at: [Link]

Business Ethics and Leadership, Volume 5, Issue 3, 2021
ISSN (online) – 2520-6311; ISSN (print) – 2520-6761

concentrate their efforts and resources (FATF, 2012)[13] to achieve the set goals and objectives for preserving the cleanliness of cross-border flows. One of the methods used by the FATF is to use categories marked with red dots after identifying the risk. In this way, the institution identifies places − sources of suspicious financial flows, from countries with high corruption risk or breach of banking secrecy, political risk for customers, and risk of products or services related to digital resources provided for management (FATF, 2007)[14]. These red dots as signs identify the threat of risk activation and their existence determines the execution of a particular transaction or ignored and verified by a suspicious transaction procedure. Identification of the initiator of the operation, the speed of the transfer and the decentralization of the system are the main factor conditions identified as prerequisites for the possibilities for cryptocurrencies to be used by those involved in activities of money laundering and terrorist financing. As criminal money laundering refers to the process by which individuals conceal the sources of illicit funds through a series of transactions before integrating them into the legal financial system.

According to E. Stavrova (2005)[15], the process of legalization − laundering of resources of criminal origin goes through four stages. The initial stage refers to the accumulation of income from illegal or tax-free income, usually through special techniques, including structuring deposits in bank accounts to avoid restrictions on cash contributions, the use of offshore banking infrastructure, or registered in offshore zone financial institutions. In the second stage of placement, transactions are carried out to break the links between illegal funds and their criminal sources. It can be very successfully achieved through transfers as payments for goods or services or as receipts from successful deliveries or the sale of goods or services. The third stage is integrating or disguising the already legalized resources to have a legal origin as they re-enter the existing financial system. It allows criminals to use their financial assets, representing income from criminal activity, with a low risk of suspicion. The fourth stage is already using financial resources for completely legal operations such as their registration as foreign direct investment, insurance benefits contracts, early repayment of loans, etc. The regulation of these clearly identified stages, efforts to build active money laundering strategies have always "followed the money movement" in attempts to establish their illegal origin of criminal activity.

Cryptocurrencies are assets whose use is constantly growing. Numerous publications are devoted to them and to the digital infrastructure, to their importance for the stability of the financial systems, examining their role, application, effects on the national economies. Ecuador − a country in Latin America, on June 8, 2021, replaced its national currency with Bitcoin, which according to the comment of Prof. Steve Hanke (2021)[16] was done by an authoritarian law with a coercive nature of replacement. According to Prof. Hanke, this is a measure with an invaluable effect since the objective value of this cryptocurrency is determined by its market value, as well as by demand and inelastic supply.

As a financial asset, cryptocurrencies have advantages and disadvantages:

- They are not threatened by inflation due to the known latest code − for example, for Bitcoin it is 21 million. And because they are not bound by monetary authorities, there are no political decisions that would change that amount for other reasons.
- The network includes all issuers − extracting and trading cryptocurrencies, without the need for a central server. Each addressee in it has a base of realized transfers, which are reflected in many contact servers.
- Decentralized information about participants and volumes − there is no database about the participants in the network, and each generating computer is already part of it. This limits the intervention of regulators to impose rules on trade and exchange.
- Anonymity of the participants in the system. Maintaining this principle also guarantees a high level of democratic access to the network and at the same time conceals participants with criminal intent.

The lack of jurisdiction that devalues already generated cryptocurrencies should be falsified and falsified. As a result, the cryptocurrency market is extremely volatile and sensitive to black swan events. High speed of transfers − transfer of assets to any point after ordering the payment in the network. This is due to the lack of an arbitrator − i.e., an institution that has once verified the digital asset and then reflects the transactions with it.

[13] FATF (2012). The FATF Recommendations: International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation. Available at: [Link]
[14] FATF (2007). Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures. Available at: [Link]
[15] Stavrova, E. (2005). Systems for prevention of the access of dirty money to the financial and credit system. ISBN 954-680-374-X, Blagoevgrad.
[16] Hanke, St. (2021). El Salvador's Big Bitcoin Mistake. Wall Street Journal. June, 22, 2021.

Although banks trade diverse assets, cryptocurrencies are a new, specific asset for which accounting theory and practice are still looking for the right way to record their transactions. Problems with treatment are essential in determining the nature of cryptocurrencies. Accounting practice faces the problem of identifying the nature of digital currencies. According to B. Brezoeva (2020)[17] cryptocurrencies can be treated in several ways:

- Cash and cash equivalents.
- Financial instrument;
- Intangible asset;
- Inventory.

According to the author, cryptocurrencies are a complex accounting object, the reflection of which is associated with significant difficulties in practice. The cryptocurrency reporting guidelines present the basic rules too vaguely in the current accounting standards, without clear regulations. It is followed by the application of a variety of accounting policies. The most common practice is to apply fair value measurement to profit or loss. The cryptocurrency held is usually associated with a foreign currency or, more generally, as a financial instrument (financial asset). A small number of manufacturers report cryptocurrency as an intangible asset or inventory. Traditionally, banks, in the process of intermediation, create money through account entries or lending; cryptocurrencies are an alternative to the decree, fiat money created by the government or the central bank and secured by assets from the national treasury. An alternative is private money created by banks that generate resources on a deposit account for the borrower in granting the loan. It means that as in financing liquidity theory n, argued by Donaldson, Piacentino and Thacor (2018)[18] and Thakor, A., Merton, R.C. (2019)[19], Thakor, A. (2019)[20], when the bank borrows, it does not have to be at the expense of available, maternity money stored in its bank vault and provide them to the borrower. The probability of lending money is higher, the bank opens a new bank deposit account, to which the borrower gets access.

Cryptocurrencies and Money Laundering or Cash Flows

The accompanying risks of cryptocurrency banking operations for financial technology operations companies are aimed at all participants in the chain of the four stages of legalization of resources of criminal origin. All large banks participate in crypto markets, make crypto-payments, and are related to the blockchain system. With the inclusion of banking institutions and FinTech companies, significant transfers in volume and, respectively, the crossing of cash flows from fiat; centralized financial assets are carried out. It is natural to examine the conditions that recreate the uniqueness of cryptocurrencies, providing our attention to the threats associated with the risks they pose to money laundering/counter-terrorism efforts. These conditions are related to the impossibility to quickly identify such red dots as a risk generator and the corresponding difficulty in applying the rules of supervision of the FATF on the operations of certain suppliers, financial intermediaries and investors in cryptocurrency.

The four-step process proves too simplistic to extrapolate to the context of digital currencies, examining the money laundering process. The first stage is the accumulation of resources that need to be legalized and obtain a legal origin. These are funds with a source of prohibited transactions in weapons, drugs, or tax evasion. Their carriers are traditionally decree or fiat currencies against which cryptocurrencies such as Coinbase or Gatehub are purchased. Another strategy is to implement this accumulation in various tokens against issued digital currencies and send them to cryptocurrencies like Binance or Bitfinex. At the third stage − for masking or integrating the thus purchased digital financial assets, transactions are concluded with marketable goods against which fiat or decree currency is again received. This is a relatively simple scheme whereby generating revenue from illicit sources can use digital resources, and by paying online, redirect their revenue to financial institutions, which give these funds a perfectly legal look. According to W. Filipkowski (2008)[21], the use of cryptocurrencies in online payments, smart cards or online banking would greatly simplify money laundering techniques and provide resources for terrorist acts compared to using the opportunities provided by the conventional banking system. If the network offers guaranteed anonymity, the speed of transactions for organizations with criminal terrorist purposes in the rapid and unrestricted movement of funds made entirely in digital currencies will ensure the successful completion of their operations. But complete anonymity is not possible because ISPs store transferred files and show the IP address from which the transfer was ordered.

[17] Brezoeva, B. (2020). Cryptocurrency − accounting challenges. Research papers UNSS, № 03, 52-76.
[18] Donaldson, J.G., Piacentino, and Thakor, An. (2018). Warehouse Banking. *Journal of Financial Economics*, *129*(2), 250-267.
[19] Thakor, R., Merton, R.C. (2019). Trust in Lending. Paper presented at the AFA Meeting, Atlanta.
[20] Thakor, A. (2019). The Purpose of Banking: Transforming Banking for Stability and Growth, Oxford University Press.
[21] Filipkowski, W. (2008). Cyber Laundering & An analysis of topology and techniques. *IJCJS, 3*.

Business Ethics and Leadership, Volume 5, Issue 3, 2021
ISSN (online) – 2520-6311; ISSN (print) – 2520-6761

Digital currencies have codes, and because their transactions are made under these unique alphanumeric combinations, providers store this output for each transfer.

Unlike transfers, which are made through settlement systems and allow for easier tracking, Blockchain is used as a record of the movement of funds, which is often extremely difficult to track in the public book. A current case in this direction is the information shared by the Blockchain site Poly Network about the breach in its security, realized by a hacker group and the largest theft of decentralized currency of 600 million USD. According to Cipter Trace (2021)[22], as a result of hacker attacks, the size of stolen cryptocurrencies has increased more than 2.8 times − from 129 million UDS in 2020 − only for the first 6 months of 2021 they are already 361 million USD. Transactions with cryptocurrencies are accompanied by some risks, which are the subject of significant research, for example, Dimitrov and others (2021).

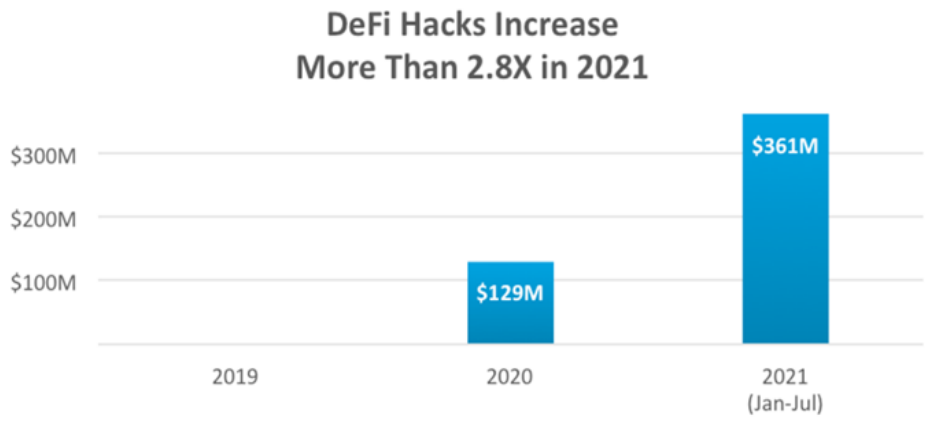

Figure 3. Dynamics of Established Attacks by Hackers on Decentralized Financial Assets

Source: CipherTrace Cryptocurency Intelligence

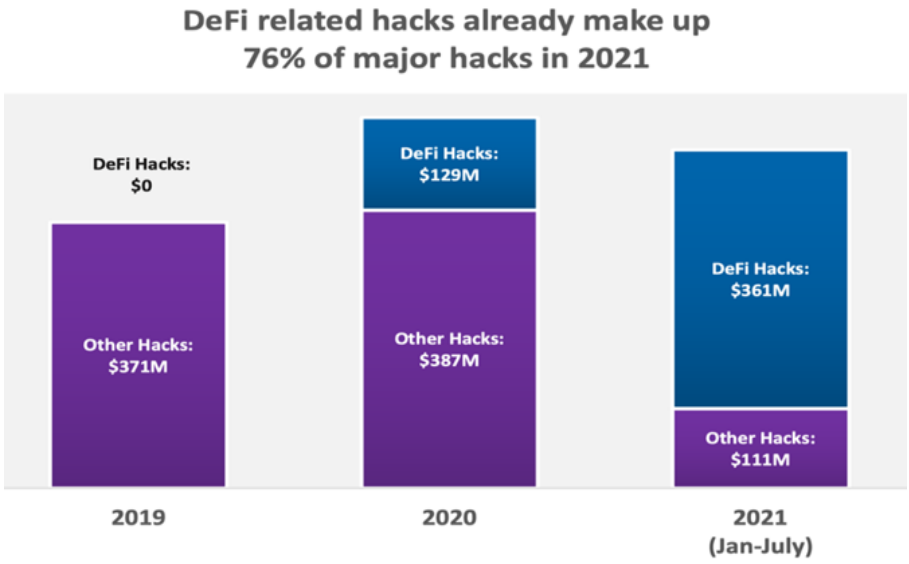

Figure 4. Share of Hacker Attacks on Decentralized Financial Assets in Relation to the Total Volume of Attacked Assets

Source: CipherTrace Cryptocurency Intelligence

The seeking legalization of financial assets truth criminal activity can choose from a variety of alternatives that can provide "possible anonymity" by "mixing" alternative cryptocurrencies with improved anonymity. The more recognizable a cryptocurrency is, the more desirable it is as a tool to achieve its goals. Due to these circumstances, some digital currencies remain largely unknown and unused (D. Carlisle, 2017)[23]. Moreover, the number of truly decentralized digital currency ecosystems is relatively small and easily assessed. Since active consumers are already customers of conventional financial and banking systems, a curious market activity from cryptocurrency transactions immediately provokes attention and it becomes monitored by the

[22] Cipter Trace (2021). Available at: [Link]
[23] Carlisle, D. (2017). Virtual Currencies and Financial Crime: Challenges and Opportunities. *Royal United Services Institute*. Available at: [Link]

institutions. It follows that there is a limited possibility of including cryptocurrencies in large and already established networks for money laundering by terrorist organizations. With the real assessment of the additional risk taken in cryptocurrencies, it is necessary to have the built capacity and readiness to apply the necessary knowledge to work in this attractive market. Hence the particular importance of following the principles of compliance procedures (N. Valkanov, E. Stavrova, 2019)[24], placed in the regulations establishing the rules for the functioning of this market.

Given the cheap nature of modern terrorist acts, there is less incentive for terrorist organizations to use the opportunities for financial gain, especially when they are risky and technically complex. Second, huge amounts of their funds "never go into the global financial system", as transactions are usually made in cash and some of their financing methods rely heavily on informal networks rather than a highly regulated international financial system. Therefore, there is little incentive for terrorism groups to start using risky and complex methods that link them to a system on which they do not depend. Given the relatively simple algorithm for organizing a modern terrorist act, the benefits for terrorist organizations to realize their plans for additional financial gains in risky and technically complex operations are unlikely to happen. Second, huge amounts of their funds are never included in global financial flows, as transactions are traditionally carried out in cash. Therefore, they rely heavily on "informal networks" and not on a highly regulated international financial system. Therefore, there is little incentive for terrorism groups to start using risky and complex methods that link them to a system on which they do not depend.

Compliance Functions of Banks in the Digital Financial Markets

The risks of violations related to the observance of the principles of ethical management of banking institutions are caused by equivalent or similar factors and the other threats in the banks' risks for which the digitization processes have introduced additional incentives. However, the effects of violating them are significantly higher when the infringement operations have deteriorated the results, such as declaring certain operations illegal and hence business restrictions or significant sanctions. For these reasons, the synchronization of the current framework for the movement of digital financial flows and compliance procedures is irrevocable and must comply with internationally recognized rules on operational risks to the world.

Integrating management mechanisms to manage functions in line with these risks offers tangible benefits.

First, they ensure that the financial institution has a truly in-depth and comprehensive assessment of the quality of its portfolio of possible risks and visibility of important systemic issues such as the use of the financial institution to enter digital financial assets to legalize criminal assets, its involvement in tax arbitrage operations with territories that are on the list of centers declared dangerous by international banking supervisors and that the supervision is designed to cover all important risks.

Second, it reduces the burden on the operating costs of financial institutions (for example, without duplicate risk assessments and elimination activities), as well as on control functions (for example, without separate or duplicate reports, training and communication activities). Third, it facilitates the allocation of enterprise resources based on risk and management actions to eliminate risk and invest in cross-sectoral controls.

The following practical actions can help the bank successfully integrate compliance into overall risk management and supervisory rules into compliance functions:

- Development of a single integrated protocol for the identification of operational and compliance risks.
- Development and centralized maintenance of standardized taxonomies for risk assessment, processes, products and control procedures.
- Coordinating the methodologies and protocols for identifying, measuring, ignoring and reporting the risks on the digital financial markets through a single comprehensive assessment of cross-border cash flows from third countries; ensuring the chronology of the activities for monitoring and testing of compliance with the activities for quality assurance or quality control in the management of operational risk.
- Defining clear roles and responsibilities between the risk and control functions of the financial institution's individual risk level to ensure that the bank has no gaps or overlaps, especially in "red areas" where the

[24] Valkanov, N., Stavrova, E. (2019). PREVENCIÓN DE FRAUDES BANCARIOS CON SEGURO DE FUNCIÓN DE CUMPLIMIENTO EFICIENTE. [Banking Fraud Prevention with Efficient Compliance Function Insurance] *100-Cs, Journal of Humanities*, 5(1), 60-71. Available at: [Link]

"

functioning of jurisdictions overlap as e.g., third country risk management, cybersecurity, international fraud.

- Development and management of joint integrated programs for training and education and communication of employees to work in a digital environment.
- Establishment and transparently defined management protocols in excess conditions and prescriptions for the work of risk management committees with powers covering the functions of cyber risk ignoring solutions, technological support to prevent hacker attacks, providing detailed and chronological reporting of operations, even if problem solving reflects on a significant part of the functions performed by financial institutions.
- Active functioning liaison and coordination of compliance efforts with government control and oversight institutions.

These new roles of financial institutions in digital markets reinforce the notion of compliance as a possible risk, too close to the operational and as a control, but not advisory function, which aims to automate and implement the integrated approach to all types of risk associated with the movement of digital financial actives. For some banking intermediaries, this has changed their cybersecurity strategy by raising compliance to the rank of an autonomous management function, equivalent in strength and importance to the internal audit. By separating it from the core business in this way, these institutions have significantly improved their vision, and at the same time, have realized the need for stronger coordination with operational risk management activities.

Conclusions

Financial flows from centralized and decentralized resources are now moving incomparably faster and easier than ever before. The technological shocks with which technology is advancing have contributed to the financial infrastructure becoming a well-functioning global ecosystem. Rapid changes involving increasing participants imply constant efforts to innovate risk management methods and regulatory compliance. By making systematic efforts in their daily work to improve technologies that deter the use of the financial system to legalize proceeds of crime or illegality, financial institutions can take advantage of emerging markets while meeting the needs of their customers and the recommendations of regulators. Compliance with the regulatory requirements for risk management from the replacement of banks in operations of money laundering of criminal origin has caused changes in their activities in various ways. The costs of this activity have realized a general increase in costs, an increase in the price of financial intermediation, and sometimes making it difficult to provide high-quality services and wonderful customer experiences as a result of this collaboration.

However, with the improvement of the regulatory environment, a significant possibility can be established for the compliance function of banking operations to outpace the curve by making important changes in the operational model and processes. Improving the quality of the supervisory activity of central banks at the same time increases the efficiency of the overall results of their activity in terms of the sustainability of the banking system. Banking systems that successfully go through this important stage − combining the processes of participation in digital financial markets with their compliance control functions inevitably get an additional opportunity for enhanced competitive advantages, improving the quality of customer service, economies of scale as a result of participation in the digital markets, to directly reduce costs and significantly reduce the risks associated with their operations.

Funding. There is no funding for this research.

References

1. Brezoeva, B. (2020). Cryptocurrency − accounting challenges. Research papers UNSS, 03, 52-76. Available at: [Link]
2. Carlisle, D. (2017). Virtual Currencies and Financial Crime: Challenges and Opportunities. Royal United Services Institute. Available at: [Link]
3. Ciphter Trace (2021). Available at: [Link]
4. Dimitrov, P., Vasenska, Iv., Koyundzhiyska-Davidkova, Bl., Krastev, Vl., Durana, P., Poulaki, I. (2021). Financial Transactions Using FINTECH during the Covid-19 Crisis in Bulgaria. *Risks*, *9*(3), 48. [Google Scholar] [CrossRef]
5. Donaldson, J., Piacentino, G., Thakor, An. (2018). Warehouse Banking. *Journal of Financial Economics 129*(2), 250-267. [Google Scholar]
6. FATF (2007). Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures. Available at: [Link]

7. FATF (2012). The FATF Recommendations: International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation. Available at: [Link]
8. FATF (2020). Financial Action Task Force. Report 2019-2020, FATF/OECD, Paris. Available at: [Link]
9. Filipkowski, W. (2008). Cyber Laundering& An analysis of topology and techniques. *IJCJS*, *3*(1), 15-27. [Google Scholar]
10. GGF (2021). Financial crime: five key trends from 2020 and how they played out. Partner Content on 22/02/2021. Available at: [Link]
11. Hanke, St.H. (2021). El Salvador's Road to Currency Chaos and Economic Collapse. Available at: [Link]
12. Hayek, Fr. (1976). The Denationalization of Money, London: Institute of Economic Affairs, 71-74. Available at: [Link]
13. Lyeonov, S.V., Kuzmenko, O.V., Mynenko, S.V., Kwilinski, A.S., Lyulyov, O.V. (2020). Determining the Rating of Ukrainian Banks on the Risk of Legalization of Illegally Obtained Income. *Механізм регулювання економіки [Mekhanism regulyuvannya economiky]*, *3*, 31-45. [Google Scholar] [CrossRef]
14. Nenovsky, N., Chobanov, P. (2021). Digital currency Vs the crypto. Bloomberg Businessweek bg. July, 2021, 44-53. Available at: [Link]
15. Rhoda Weeks-Brown (2019). Cleaning Up. Countries are advancing efforts to stop criminals from laundering their trillions. Available at: [Link]
16. Stavrova, E. (2005). Systems for prevention of the access of dirty money to the financial and credit system. ISBN 954-680-374-X, Blagoevgrad, 48-53.
17. Thakor, R., Merton, R.C. (2019). Trust in Lending. Paper presented at the AFA Meeting, Atlanta. Available at: [Link]
18. Thakor, A. (2019). The Purpose of Banking: Transforming Banking for Stability and Growth, Oxford. University Press. ISBN 0190919531, 9780190919535. 256 p. [Google Scholar]
19. Thakor, Anjan V. (2019). Fintech and banking: What do we know? *Journal of Financial Intermediation*, *41*, 100833. [Google Scholar] [CrossRef]
20. Tommaso, F.D. (2020). The New Italian Legislation on Corporate Governance and Business Crisis. The Impact of Covid–19 on SMEs and the Recent Rules to Mitigate the Effects. *Financial Markets, Institutions and Risks*, *4*(4), 91-108. [Google Scholar] [CrossRef]
21. Valkanov, N., Stavrova, E. (2019). Prevención de fraudes bancarios con seguro de función de cumplimiento eficiente [Banking fraud prevention with efficient compliance function insurance]. *100-Cs, Revista de humanidades* [Journal of Humanities], *5*(1), 60-71. Available at: [Link]
22. Vasilyeva, T., Sysoyeva, L., & Vysochyna, A. (2016). Formalization of factors that are affecting stability of Ukraine banking system. *Risk governance & control: financial markets & institutions*, *6*(4), 7-11. [Google Scholar] [CrossRef]
23. Vasylieva, T.A., Lieonov, S.V., Letunovska, N.V. (2019). Financial, business and trust cycles: the issues of synchronization. *Zbornik radova Ekonomskog fakulteta u Rijeci*, *37*(1), 113-138. [Google Scholar] [CrossRef]
24. Zolkover, A.O., Georgiev, M. (2020). Shadow Investment Activity as a Factor of Macroeconomic Instability. *Financial Markets, Institutions and Risks*, *4*(4), 83-90. [Google Scholar] [CrossRef]
25. Zlateva, D., Stavrova, E., Vladov, R. (2017). Digital Bank Marketing in the Context of the Circular Economy. *International Journal for Science and Arts − "IDEA"*, *1*(1), 31-38. Available at: [Link]