Laundering of Criminal Proceeds Through Cryptocurrency Transactions: A Digital Threat to Economic Security

Submitted: 23 December 2023
Reviewed: 17 February 2024
Revised: 19 February 2024
Accepted: 22 February 2024

Article submitted to peer blind review

Dmitriy Kamensky[*]
https://orcid.org/0000-0002-3610-2514
Andrii Chernyak[**]
https://orcid.org/0000-0002-4958-783X
Oleksandr Dudorov[***]
https://orcid.org/0000-0003-4860-0681
Igor Fedun[****]
https://orcid.org/0000-0002-1012-9970
Serhii Klymenko[*****]
https://orcid.org/0009-0004-2629-2133

DOI: https://doi.org/10.26512/lstr.v16i2.52003

Abstract

[Purpose] The purpose of this study is to discuss, based on international as well as national laws and practices, various issues and potential solutions surrounding the growing problem of money laundering practices using cryptocurrency transactions.

[Methodology] A balanced combination of theoretical and empirical methods has been used in the course of research; in particular, the method of comparative legal research has been employed extensively throughout the text of article.

The theoretical component of this research paper includes commentaries by Ukrainian, German, other European as well as American researchers in this field. Their works are cited appropriately. The subject scope of the paper covers modern phenomenon of money laundering based on cryptocurrency transactions.

[Findings] This paper extensively discusses international and national legal frameworks for identifying and stopping as well as preventing various money laundering schemes and

[*]Doctor of Law, Professor. Dmitriy Kamensky is a professor at criminal law and criminology department at the National Academy of Security Service of Ukraine. He holds an LL.M. in Taxation degree from Georgetown University (Washington, D.C., USA). E-mail: dm.kamensky@gmail.com.

[**]Doctor of Law, Professor. Professor Chernyak works at the National Academy of Security Service of Ukraine. E-mail: ironsteel1997@gmail.com.

[***]Doctor of Law, Professor. He is professor of the department of criminal law policy and criminal law of the educational and scientific institute of law at Taras Shevchenko National University of Kyiv, Ukraine. E-mail: o.o.dudorov@gmail.com.

[****]Doctor of Economics and professor of the department of financial and economic security at the National Academy of Security Service of Ukraine. E-mail: fil_2604@ukr.net.

[*****]PhD in Law, Associate Professor. Serhii Klymenko is the head of the criminal law and criminology department at the National Academy of Security Service of Ukraine. E-mail: serklymenko@gmail.com.

techniques based on cryptocurrency transactions and blockchain technology in general. It has been established that with the global cryptocurrency market valued at roughly $1 trillion, its attractiveness to money launderers endangers economies and financial systems of numerous world jurisdictions. Based on theoretical observations and relevant analyses of legal cases, authors' conclusions on how to fight this latent type of criminality have been presented.

[Practical Implications] The research is deemed to be of value to national regulators, law enforcement agents and legal commentators, who think, write and act with the goal of fighting new money laundering patterns. It can serve as part of a broader international roadmap on how to identify suspicious money laundering schemes using various cryptocurrency transactions and also to impose effective sanctions on criminal actors behind those schemes.

[Originality] The paper originality relies on its comprehensive and balanced combination of economic and legal analyses of the issues presented and potential solutions to them. It also incorporates both sound theoretical research and in-depth coverage of law enforcement actions, as well as legal cases against crypto money launderers.

Keywords: Money Laundering. Cryptocurrency. Economic Security. Criminal Offense.

INTRODUCTION

Protection of national economic interests requires introduction of a strategic course in the field of economic security aimed at both sustainable increase of competitiveness of national economy and gradual strengthening of economic stability and invulnerability of the national economy to various external and internal threats.

This is even more important given the globalized nature of modern markets as well as emerging threats to global economic security. As a result of globalization, markets and other non-state entities become increasingly important actors in national politics and economy. Indeed, modern commerce has transcended territorial definitions and is now extra-territorial and global in its nature, as capital, technology, and investment routinely cross-national borders (KAMENSKY, 2021). The factor of globalization is even more evident when we look at money laundering schemes based on various virtual currency transactions.

When committing money laundering of crime proceeds, the economy, especially in its modern, digitalized capacity, suffers the greatest damage. As a result of laundering, a significant part of its components, including macroeconomic, financial, foreign economic, investment and production, are undermined. The negative impact of legalization is not limited just to economic sphere; the most obvious consequence of money laundering is damage caused by predicate offenses and the increase in the illegally obtained income. Other threats are no less dangerous, such as the growth of corruption, the rise of drug trafficking and other "street" crime, also organized crime, and the increase of economic and

political influence by money laundering syndicates. All this leads to the undermining of the political institutions of the state (DUDOROV & TERTYCHENKO, 2015).

In Ukraine, as a typical case for many jurisdictions, the state anti-money laundering policy is based on this country's international legal obligations and the interests of protecting national economy from illegal schemes. In adhering to international standards, any state governed by the rule of law must take into account specifics of their implementation, taking into account the national legal system and specific socio-economic conditions. This determines the vector of solving the issue of finding a balance between compliance with international standards and consideration of one's national interests (HONCHARUK, 2021).

Money laundering is anything but a new phenomenon. However, if the infamous mafia kingpin Al Capone, who, through the use of a network of purchased laundries and other businesses, essentially coined the term "money laundering," (SANCTION SCANNER, 2023) could have a look at our current reality, he would probably be astonished at how efficiently "crypto-laundries" operate in the 21st century. Virtual currencies, such as Bitcoin, Ethereum, and Ripple, are digital equivalents of value that, like fiat currency, function as a medium of exchange, unit of account, and store of value. While virtual currency enthusiasts tout their technological promise, many researchers argue that the anonymity offered by such new financial instruments makes them a very attractive tool for money laundering. As a result, law enforcement, regulators, and courts have hard time trying to figure out how virtual currencies "fit" into the anti-money laundering (AML) legal regime, which is designed primarily for traditional financial institutions (VIRTUAL CURRENCIES AND MONEY LAUNDERING, 2019).

In the comparative context, despite the fact that the Law of Ukraine of February 17, 2022 "On Virtual Assets", which should regulate the legal status of cryptocurrencies[1] in Ukraine, has not yet entered into force (due to the binding of cryptocurrency market launch to the introduction (still at works) of the procedure for taxation of transactions with virtual assets), the crypto asset market is growing steadily in Ukraine, which has become one of the world leaders in the use of crypto assets (KHOMENKO, 2023). Penetration of virtual assets into global

[1]For the purposes of this article, the terms "virtual asset", "virtual currency" and "cryptocurrency" are considered synonymous. At the same time, at least under Ukrainian law, the normative definition of the concept of a virtual asset as an intangible good that is the object of civil rights, has a value and is expressed by a set of data in electronic form (Article 1 of the Law of February 17, 2022), allows this concept to include other intangible goods, which are distinct from cryptocurrency, as well.

finance, their various combinations with fiat (classical) money, raise security and regulatory issues (KOSHOVYI, 2023).

Integration of economic systems of many countries, digitalization of the economy, emergence of new financial instruments, development of high technologies – these factors may have a "flip side" and can be used not for legal purposes only. In today's environment, cryptocurrency transactions are often used for money laundering, as such transactions make it difficult to identify persons who commit them. Bitcoin, for example, can be used to implement a variety of laundering schemes that virtually block the possibility of identifying the perpetrator (DYNTU & MITROFANOV, 2017).

Among some advantages of cryptocurrencies, which also makes them attractive for money launderers, are:

1) They are decentralized and not controlled by any central authority, which means they are less vulnerable to censorship, corruption, or manipulation;
2) They offer a high level of security and privacy, as transactions are encrypted and verified by a network of nodes, and users can remain anonymous or pseudonymous;
3) They are transparent and immutable, since all transactions are recorded on a public ledger that cannot be altered or erased. This ensures trust and accountability among users;
4) They are diverse and innovative, as there are thousands of different cryptocurrencies with different features, functions, and areas of usage. Users can freely choose the ones that suit their specific needs and preferences (KOIRALA, 2021).

A virtual currency transfer usually includes a message about identification data (sender, recipient, digital document) and the amount of currency transferred. The key obstacle for law enforcement is that such transactions can be carried out using anonymous addresses/identities and they are often encrypted. One person may use several different identities/addresses on a single platform. Since virtual currency transactions are conducted online, they leave little or no documented evidence at all (RICHARDSON & DE LUCAS MARTIN, 2021).

Given the transnational (indeed global) nature of money laundering, especially when committed with the help of virtual assets, international cooperation in combating this crime is of particular importance (DUMCHIKOV, 2022). Countering money laundering requires understanding of the nature and factors behind this socially dangerous phenomenon, as well as appropriate legal support in accord with strict international standards and practices (ZAKHAROV,

2014). Therefore, research aimed at studying progressive foreign experience in counteracting modern money laundering schemes, including through cryptocurrency transactions, is quite relevant.

RESULTS

On the Scale and Specifics of the Cryptocurrency-Based Money Laundering

It is quite difficult to estimate the global volume of money laundering (not least because of the latency of the relevant offenses, their complex and multi-episodic nature), but it remains significant in any case. Thus, according to the United Nations Office on Drugs and Crime (UNODC), 2 to 5% of the world's GDP is laundered annually, which amounts to 715 to 1.87 trillion euros (MONEY LAUNDERING). Today money laundering is a global industry as part of the black market and is worth up to $225 billion. The Europol expert report estimates that 0.7 to 1.28% of the total European Union's (EU) annual GDP is involved in suspicious financial activities, especially money laundering (EUROPOL, 2017). We are talking about billions of euros of "dirty" money within one of the most economically powerful and transparent regions of the world.

Based on some expert estimates, in 2022 alone nearly $23.8 billion worth of cryptocurrencies were transferred through illegal email addresses (i.e., without monitoring of transactions). Several major centralized exchanges were among the largest recipients of illegal cryptocurrency, receiving slightly less than half of all funds sent from suspicious crypto wallets. This is noteworthy not only because such cryptocurrency platforms typically have strict compliance measures in place to report suspicious activity and take action against questionable users, but also because crypto exchanges have various conversion services, which allow illegally obtained or previously "laundered" cryptocurrency to be converted into cash (CRYPTO MONEY LAUNDERING, 2022).

Based on the expert estimates by the authoritative analytical resource *Chainalysis*, in 2021 the total amount of funds in cryptocurrencies obtained as a result of illegal actions was approximately 18 billion dollars, and in 2022 – over 20 billion dollars (see the Chart). At the same time, despite such high absolute indicator, the volume of illegal operations constitutes only about 0.15% of total cryptocurrency transactions per year (2023 CRYPTO CRIME TRENDS).

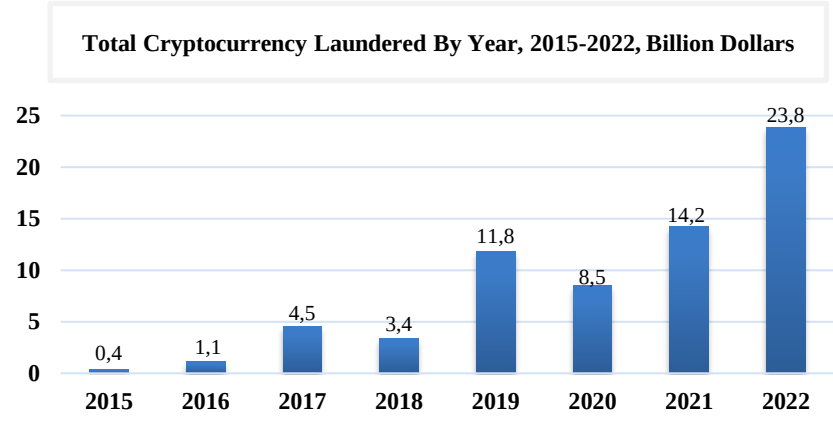

Chart 1 – Total Cryptocurrency Laundered by Year 2015 - 2022

When cryptocurrencies, crypto-exchanges, smart contracts, electronic wallets and other related tools and technologies are used for money laundering purposes, we are talking about the stages of placement and concealment: criminals seek to "separate" cash or non-cash funds from their sources of illegal origin as soon as possible by converting them into one or more cryptocurrencies, and then hiding them from state monitoring and detection through a series of complex and chronologically long operations in the virtual world. At the same time, given their high volatility and profitability, the owner (beneficiary) of virtual assets often does not use the third stage – integration in the form of exchanging cryptocurrency for fiat currency or other financial instruments for further investment in legal sectors of the economy. Such person is quite satisfied with the "depository" nature of control over crypto assets as a modified form of property previously obtained by criminal means. In addition, due to high possibility of fast exchange rates growth, when some cryptocurrencies demonstrate a rapid increase in value, it is easy to justify (explain) unexpected excess profits through the possession of cryptocurrencies. It takes just a few seconds to create an account ("email address") for storing and trading cryptocurrencies, and in most cases, it is free and anonymous. It is also possible to create a large-scale laundering scheme with thousands of low cost and high speed transfers by executing it (the scheme) using a predefined algorithm.

Among various methods of money laundering based on cryptocurrency transactions, used by criminal actors, the most common are the following two.

1) **Privacy coins.** These are cryptocurrencies that offer a higher level of anonymous transactions on the blockchain, which makes the currency even less traceable than "regular" cryptocurrencies. A higher level of anonymity can be achieved, for example, by hiding information about users' addresses from third parties. This contrasts with the way so-called "regular" cryptocurrencies (such as Bitcoin, Ethereum, Binance Coin, XRP, Solana) work, where anybody can see the balance of a crypto wallet as well as transactions between virtual addresses.
2) **Crypto-mixers.** The global cryptocurrency market is currently actively using several technologies, which allow to "mix" potentially identifiable cryptocurrency funds in order to conceal their source of origin, thus making it impossible to track them down. Cryptocurrencies from several sources are first sent to one virtual address (account). After funds have been randomly "mixed" at this address, they are further divided into several parts and sent to different addresses. To ensure greater degree of secrecy, this process can be repeated several times over before funds finally reach their destination. As a result, it is virtually impossible to trace funds received by the beneficiary to their source (MONEY LAUNDERING THROUGH CRYPTOCURRENCIES, 2024).

The above-mentioned features create an almost ideal basis for "crypto-legalization". In order to address the increased risks, the UNODC is currently implementing its own analytical project aimed at studying cryptocurrencies as a new means of money laundering and developing recommendations to counter such practices (MONEY LAUNDERING THROUGH CRYPTOCURRENCIES, 2024).

In our increasingly digitalized and economically integrated world, an important question arises: can technologically innovative virtual currencies complicate financial monitoring and anti-money laundering measures by national regulators and law enforcement agencies? So far, the answer to this question is, unfortunately, yes.

International Legal Regulation of Anti-Money Laundering through Transactions with Virtual Assets

Introductory part of Directive (EU) 2018/843 of the European Parliament and of the Council of May 30, 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (commonly known as Anti-Money Laundering and Terrorist Financing Directive (AMLD V); hereinafter referred to as Directive (EU) 2015/849) states that at the

time of adoption of this document, providers of exchange services between virtual and fiat currencies (i.e. coins and banknotes that are legal tender and electronic money of a country as a means of exchange in the issuing country), as well as providers of electronic wallets in the EU countries, were not required to detect suspicious activity in cryptocurrency transactions. As a result, terrorist groups could transfer money into the EU financial system or within virtual currency networks, thus effectively concealing such transfers or using a certain degree of anonymity. Accordingly, the question was raised about expanding the scope of Directive (EU) 2015/849 to cover persons providing exchange services between virtual and fiat currencies, as well as providers of electronic wallet administration services. It was also emphasized that, for the purposes of combating money laundering and terrorist financing, competent authorities should be able to monitor the use of virtual currencies through authorized persons. It was expected that such monitoring would ensure a balanced and proportionate approach, while protecting technological progress and a high degree of transparency in the field of alternative finance and social entrepreneurship (DIRECTIVE, 2018).

In order to increase the level of transparency in the European financial ecosystem, Directive (EU) 2015/849 introduced, among other things, stricter requirements in terms of:

1) Establishing publicly accessible registers for companies, trusts and other legal arrangements;
2) Strengthening powers of the EU financial intelligence units and providing them with access to extensive information to fulfill their tasks;
3) Limiting anonymity associated with virtual currencies and virtual currency wallet providers, as well as for prepaid bank cards;
4) Expanding the criteria for assessing high-risk third countries and improving safeguards for financial transactions to and from such countries;
5) Improving mechanisms for cooperation and information exchange between anti-money laundering supervisory authorities, as well as between them, prudential supervisors and the European Central Bank (EU CONTEXT OF ANTI-MONEY LAUNDERING, 2023).

Directive (EU) 2015/849 authorizes national financial intelligence units to obtain information which allows them to link virtual currency addresses directly to the identity of the virtual currency owner (HAFFKE ET AL., 2020). In its part, in October of 2018 the Financial Action Task Force on Money Laundering (FATF) amended its Recommendations to formally state that they also apply to financial activities related to virtual assets. At the same time, two new terms were

added to the FATF glossary – "virtual assets" and "virtual asset service provider" (VASP). Recommendation 15 sets out requirements that VASPs should be subject to anti-money laundering and countering financing of terrorism (AML/CFT) regulation, licensing or registration, and should be subject to effective control or supervisory systems.

In September of 2020, the FATF presented the report "Money Laundering and Terrorist Financing Threat Indicators Related to Virtual Assets". Based on the study of over one hundred cases collected by the FATF staff, this document highlights the most important features (indicators) which may indicate illegal behavior of transaction participants. The main indicators described in the analytical document include:

1) Technological features that enhance anonymity (use of peer-to-peer exchange websites, crypto asset mixing or blending services, or use of cryptocurrencies with enhanced levels of anonymity);
2) Geographic location risks: criminals may use countries with weak or non-existent models of control over virtual assets;
3) Transaction patterns – conducting transactions with cryptocurrency in an irregular, unusual or illogical manner, which may indicate signs of criminal activity;
4) Transaction size (if the amount and frequency of transactions have no logical economic explanation);
5) Sender or recipient profiles – unusual behavior may indicate potentially criminal activity;
6) Sources of origin of funds or other assets – the presence of indicators of misusing various virtual assets, which often relates to criminal activities, such as illicit trafficking in narcotics and psychotropic substances, fraud, theft and extortion (including cybercrimes).

The report is intended, among other things, to serve as a source of useful information for financial intelligence units, law enforcement agencies, prosecutors and regulators to analyze suspicious transaction reports or monitor compliance by obligated entities with anti-money laundering and counter-terrorist financing measures (FATF, 2020).

On July 20, 2022, FATF issued a report "Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing" (FATF, 2022). The background for issuing such analytical document relies on the fact that a single financial institution possesses only a partial perspective on transactions, thus capturing just a small fragment of what is often a complicated puzzle. Criminals exploit this information gap by leveraging

multiple financial institutions within or across jurisdictions, which allows them to intricately layer their illicit financial flows. In order to address this issue, financial institutions are turning to collaborative analytics, by combining data or initiating sharing endeavors responsibly. This FATF report was drafted with the goal of guiding national jurisdictions in responsible enhancing, designing, and implementing collaborative information initiatives among private sector entities. It emphasizes compliance with data protection and privacy (DPP) rules to ensure that risks associated with increased sharing of personal data are prudently addressed.

By examining global anti-money laundering, counter-terrorist financing, and counter-proliferation financing requirements, the report explores how responsible private-to-private collaboration can contribute to their effective implementation. Additionally, it introduces the DPP principles and objectives that stakeholders should consider when designing private sector collaboration initiatives, thus emphasizing their importance. Based on multiple case studies, the report illustrates how FATF members and its Global Network have enhanced private sector information sharing within the legal requirements of their domestic DPP framework. These experiences underscore the fact that private sector information sharing measures can align with DPP rules and obligations, subject to key tests and requirements.

According to Krik Guning, CEO of "Fourthline", a financial consulting and background check firm, in order to create a safer financial ecosystem, the global financial industry has to leverage technology and also to actively promote cross-border cooperation between private and public sectors (JOINING FORCES, 2023). This is even more important today with the fight against financial crime, which is becoming more challenging as the world becomes increasingly digital, and financial crime remains roughly a $2 trillion issue.

One might expect that enhanced data sharing practices, provided for in the 2022 FATF report, will also contribute to the ongoing law enforcement initiatives to fight cryptocurrency schemes used to launder illicit funds. After all, transparency and accountability in everyday activities of financial institutions and cryptocurrency exchanges are key to successful combatting money laundering schemes on a global scale.

Several jurisdictions have just recently started taking the issue of crypto money laundering seriously. Brazil is one of them. The cryptocurrency regulation, which was approved by the Brazilian congress at the end of 2022, has become law in July of 2023, thus marking a potential move towards comprehensive sector-specific legislation. The central bank was designated by the Presidential decree as the primary overseer of the crypto economy – such official move positions the central bank to supervise and regulate all virtual asset providers in the country.

Industry experts are optimistic that this step could serve as a pioneering model for the global cryptocurrency regulation (FELIBA, 2023).

More criminal cases related to crypto laundering schemes have been recently opened in Brazil, which is quite illustrative of the "tough on crime" global approach to fighting this emerging type of white-collar crime. As just on example, in January of 2024, the Brazilian Federal Police apprehended an individual suspected of laundering substantial sums, exceeding $2.6 billion, derived from drug trafficking and other criminal activities through the use of cryptocurrency assets. The illicit enterprise facilitated the flow of funds through accounts held by shell companies under control of the suspect. The arrest took place at São Paulo International Airport, where the individual was apprehended while en route to Dubai. The investigation revealed that the suspect acquired illicit funds in Brazil, converted them into cryptocurrency, and then directed them through various shell company accounts. Notably, one of these companies recorded transactions totaling $285 million within a 10-month period, none of which was reported to tax authorities (CARILLO, 2024).

Relevant American Experience in Combatting money Laundering Schemes Based on Cryptocurrency Transactions

Today, countering money laundering practices committed through the use of cryptocurrencies is becoming especially relevant for the United States as a global economic driver and leader of digital technologies sector.

> "The United States has a comprehensive and technology-neutral regulatory and supervisory system to regulate and supervise digital financial assets in the area of anti-money laundering and countering terrorist financing. This means that virtual currency service providers and their activities are subject to the same regulation as non-digital asset service providers, i.e., they are subject to a common regulatory framework... the United States supervises any person engaged in the business of accepting and transferring monetary value, regardless of whether it exists in physical or digital form"[2].

On November 21, 2023 the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN)[3] has taken unprecedented legal action to

[2] Perepelitsya, M. O. (2021). Virtual Currency as an Object of Financial Monitoring: Taking into Account the Experience of Foreign Countries in the Formation of National Legislation. Law and innovation, 2, 58-66.

[3] The mission of the Financial Crimes Enforcement Network, as a separate division of the U.S. Department of the Treasury, is to protect the financial system from illicit use, combat money laundering and related crimes, including terrorism, and promote national security through the strategic use of financial agency resources and the collection, analysis and dissemination of operational and analytical materials of financial intelligence.

hold Binance Holdings Ltd. and several of its subsidiaries (collectively – Binance[4]) accountable for violating U.S. anti-money laundering (AML) laws and sanctions laws designed to protect the U.S. national security and the integrity of the international financial system. Binance's management entered into a settlement agreement with the FinCEN and the Office of Foreign Assets Control (OFAC, another division of the U.S. Department of the Treasury) for violations of the Bank Secrecy Act and apparent violations of several governmental programs for the application of international economic sanctions. Violations included failing to implement programs to prevent suspicious transactions with terrorists, including al-Qassam Brigades of Hamas, Palestinian Islamic Jihad, al-Qaeda, and the Islamic State of Iraq and Syria (ISIS), and failing to report suspicious transactions with terrorists, money launderers, and other criminals. It also involved transactions between crypto-exchange participants in the United States and users in several sanctioned jurisdictions, such as Iran, North Korea, Syria, and the Autonomous Republic of Crimea in Ukraine. By failing to comply with its anti-money laundering and sanctions obligations, Binance allowed a number of entities to make apparently illegal transactions on its platform.

The settlement has become a part of a global agreement concluded by Binance with the U.S. Department of Justice (DOJ) and the Commodity Futures Trading Commission (CFTC). The agreement between the crypto exchange and FinCEN includes a $3.4 billion civil penalty and five years of probationary compliance monitoring, as well as significant compliance obligations, including ensuring Binance's complete exit from the US market. The settlement agreement with the U.S. Treasury Department's OFAC provides for a fine of $968 million and requires Binance to comply with a number of stringent compliance obligations, including full cooperation with FinCEN's monitoring authorities. To ensure that Binance complies with the terms of the settlement, including that it will not offer services to U.S. citizens, and to ensure that its illegal activities are disrupted, the U.S. Treasury Department will retain access to Binance's books, records, and systems for five years (U.S. TREASURY, 2023).

As an important component of the state anti-money laundering mechanism, § 1956 and § 1957 of the US Criminal Code are federal criminal law provisions aimed at combating money laundering. These provisions, which prescribe elements of four offenses depending on the type of illegal transactions (financial (banking) transactions; physical movement of assets; use of financial institution instruments; money transactions (transfers)), are formulated so broadly that courts usually have no issues while applying them to new 'digital legalization' schemes (18 U.S. CODE § 1956).

[4] Binance is the world's largest virtual currency exchange, responsible for approximately 60% of centralized spot trading of these assets.

In order to prosecute under § 1956 of the U.S. Criminal Code, it is necessary to establish that the financial transaction included: 1) the transfer of funds by electronic or other means, or 2) the use of one or more monetary instruments that in some way affect business financial relations at the state or national level (TOWNSEND, 2001). The defendant must be aware that the assets which are the subject of the transaction were obtained in whole or in part by criminal means, namely as a result of a felony (serious crime). § 1956(c)(7) of the U.S. Criminal Code sets forth a list of criminal acts which may result in the formation of illegal funds and instruments. This list includes various federal and state crimes, such as bribery, export violations, other economic crimes, and crimes against the established order of drug trafficking.

Within the outlined boundaries of our discussion, we will refer to the following high-profile sanctions case.

On November 3, 2023 the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed financial and administrative sanctions on Russian citizen Ekaterina Zhdanova for using cryptocurrency with the purpose of money laundering in the interests of Russian elites. According to OFAC, in March 2022, she helped a Russian client legalize over $2.3 million by transferring money to Europe through the use of fraudulent investment accounts and real estate transactions. In another episode, a Russian oligarch contacted Zhdanova to transfer approximately $100 million to the United Arab Emirates (UAE). She also helped him and similar clients to obtain tax residency status in the UAE, as well as identification cards and bank accounts. The defendant used similar tactics to move illegally obtained funds for the Russian ransomware group Ryuk. The funds were transferred through crypto platforms without any anti-money laundering and counter-terrorist financing (AML/CFT) clearances. One of such platforms is Garantex, a Russian crypto exchange banned by OFAC, which accounts for the majority of transactions related to the sanctions imposed in 2022-2023. The defendant also used her connections with other money launderers to expand her global network and gain access to more traditional respectable businesses, such as a premium watch company, which, in turn, allowed her to get access to financial systems of other countries (TREASURY, 2023).

Ekaterina Zhdanova was included in the sanctions list according to the decree of the President of the United States "Blocking property due to certain harmful foreign activities of the government of the Russian Federation" – for her participation in money laundering on behalf of Russian oligarchs and Russian ransomware groups. The mentioned document provides for an administrative sanction in the form of blocking any tangible and intangible assets (including any accounts and other financial instruments) under the jurisdiction of the United States for actions related to direct or indirect participation in deceptive or

structured transactions or operations to circumvent any United States sanctions, including through the use of digital currencies or assets or the use of physical assets, on behalf of or for the benefit, directly or indirectly, of the Government of the Russian Federation (EXECUTIVE ORDER, 2021).

As an observation remark, American authorities are implementing a comprehensive legal response to suspicious transactions, which use cryptocurrencies. The U.S. experience is both interesting and disturbing; it also reveals that the use of virtual assets for money laundering is not some kind of autonomous phenomenon, but a rather important component of cybercrime. Its scale in today's ever more digitalized world is impressive, while leading to serious concerns.

Countering Crypto Laundering: Ukrainian Dimension

Just as the war of aggression against Ukraine has united many nations around the world, including law enforcement and judiciary (KAMENSKY, 2022), the Ukrainian economy also remains connected to the global markets, which is a positive trend.

Ukraine has acceded to two fundamental international acts designed to provide a systematic approach to countering legalization schemes. They are: The Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of November 8, 1990, ratified by Ukraine on December 17, 1997 (Strasbourg Convention); the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the Financing of Terrorism of May 16, 2005, ratified by Ukraine on November 17, 2010 (Warsaw Convention). Article 20 of the Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their Member States, on the other, refers to the strengthening of cooperation in the field of preventing and combating money laundering and terrorist financing. To this end, Parties shall ensure implementation of relevant international standards, in particular FATF standards and standards equivalent to those adopted by the EU.

Article 16 of the Law of Ukraine "On Digital Assets" (THE LAW OF UKRAINE, 2022) provides that state regulation of the virtual assets market is based on the implementation by the state, represented by the National Securities and Stock Market Commission (NSSMC) and the National Bank of Ukraine (NBU), of comprehensive measures to streamline, control, and supervise the virtual assets market, regulate rules of operation of service providers related to the turnover of virtual assets, as well as measures to prevent and counteract abuse and violations in the virtual assets market. Thus, the NSSMC: 1) controls and supervises compliance by virtual asset market participants (except for a secured virtual asset, i.e. the one that certifies property rights, including the right to claim other civil rights) with the

legislation on virtual assets and brings them to justice for violations of such legislation; 2) forwards legal materials based on the facts of potentially administrative or criminal offenses to competent law enforcement agencies. As a result, the NSSMC should by its legislative design exercise powers of the state financial monitoring entity with respect to service providers related to the circulation of virtual assets. As one might see, there are some similarities in the powers of cryptocurrency regulation between Ukrainian and American stock market regulators in this regard.

On the one hand, adoption of the Law "On Digital Assets" indicates Ukraine's desire to actively join global (through UNDOC, Interpol) and pan-European (through FATF, MONEYVAL) trends in effective legal regulation of the cryptocurrency market, in particular to counteract practices of using such assets for illegal purposes, including money laundering. On the other hand, inconsistent practices by the national legislator on the issue of which state body should be responsible for the relevant financial monitoring clearly does not contribute to the effective counteraction to money laundering committed through transactions with virtual assets. "At the current stage of financial monitoring practices in Ukraine, it is important to ensure the effectiveness of interaction between financial monitoring entities, develop transparent criteria for identifying transactions with virtual assets subject to financial monitoring, and mechanisms for transferring information about such transactions" (OVCHARENKO, 2020).

On the domestic cryptocurrency enforcement front, the National Anti-Corruption Bureau of Ukraine (NABU) has been learning methods of tracing illegal assets and studying tools of new types of corruption, with cryptocurrency technologies among such tools. Forensic technologies such as Crystal blockchain (CRYSTAL SCHOOL, 2023) help to: 1) identify suspicious transactions and relationships between wallets; 2) provide means to identify and analyze transactions that may be related to money laundering; 3) identify transactions and addresses associated with terrorist groups or ongoing criminal enterprises; 4) assist in the investigation of suspicious activity by providing detailed information about transactions, including geographic distribution, IP addresses used, and various other metadata (BEREST, 2023).

Understanding the blockchain technology itself is crucial for law enforcement investigations. A blockchain operates as a distributed database or ledger that is shared among nodes within a computer network. Its prominent role in cryptocurrency systems involves maintaining a secure and decentralized record of transactions, yet its applications extend beyond cryptocurrency. While diverse types of information can be based on a blockchain, its primary use has been for transactions, serving as a ledger.

Since the introduction of Bitcoin in 2009, the use of blockchain has expanded significantly, giving rise to various cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts. The immutability of

decentralized blockchains means that once entered, data becomes irreversible; for Bitcoin, for example, transactions are permanently recorded and accessible to all (HAYES, 2023).

In 2022, the State Financial Monitoring Service of Ukraine prepared a detailed report on the legislation on regulation of virtual assets in the areas of anti-money laundering and counter-terrorist financing (REVIEW OF THE LEGISLATION, 2022). This document covers in detail the anti-money laundering practices based on transactions in virtual assets in various jurisdictions across the globe.

It should be emphasized, however, that money laundering through cryptocurrency transactions should be distinguished from the predicate offense committed with the use of new tools designed to conceal the criminal source of income. For example, virtual currency can be used to ensure anonymity when purchasing things like drugs or firearms (RICHARDSON, I. & DE LUCAS MARTIN, 2021). "By using cryptocurrency payments, the offender removes himself as much as possible from contact with the potential buyer, leaves minimum traces of the criminal act, and by excluding visual contact and communicating through Internet messengers, significantly complicates detection and investigation of this type of crime." The use of virtual assets and blockchain technology for money laundering is neither about the origin of the property, nor about the acquisition, possession, use, or disposal of property mentioned in Article 209 of the Criminal Code of Ukraine. Instead, it is the use of virtual assets to change the form (transformation) of property of criminal origin or to commit actions aimed at concealing, disguising the origin of such property or possession of it, the right to such property, or the source of its origin, which is equally punishable under this criminal law provision.

Correctness of the above thesis is confirmed, in particular, by the domestic practice of seizing crypto assets belonging to persons suspected of committing corruption offenses. As one recent example, in November 2023, the NABU and the Special Anti-Corruption Prosecutor's Office secured the seizure of USD 1.55 million in crypto assets found on the property of the former head of the State Service for Special Communications and Information Protection of Ukraine, who is suspected of misappropriating over UAH 62 million in budget funds allocated for the purchase of equipment and software. The High Anti-Corruption Court of Ukraine upheld the relevant motion and seized such crypto assets, as Tether USDT in the amount of 1.2 million units ($1.2 million at the time of the exposure), TRX in the amount of 331 units ($35,000) and 6.9 bitcoins ($275,000) (DYACHKINA, 2023). One might assume that this government official has laundered stolen funds by transferring them into cryptocurrency.

Overall, both American and Ukrainian (and probably elsewhere) approaches reveal that cryptocurrencies appeal to the criminal world because they are based on a decentralized and blockchain system: electronic money is free and

not regulated by any financial authority in any country, and system users are both anonymous and exercise equal rights (DUMCHIKOV et al., 2022). Cryptocurrency has both pros and cons, with the biggest of the latter probably being its lack of transparency and its many options for money laundering.

CONCLUSIONS

Anti-laundering legislation is an extremely mobile, ever shifting regulatory and sanctioning matter, with money laundering itself being an extremely negative phenomenon for the global economy. Money laundering through the use of virtual currencies is nowadays a significant, though hardly the last, stage in the long-running confrontation between the state, represented by law enforcement and regulatory authorities, on the one hand, and representatives of the criminal world, on the other. Digital reality of today's world, which is actively transforming public life, also creates new challenges in the field of anti-money laundering, requiring state institutions to take timely and strict measures of unprecedented nature.

The criminal law of Ukraine, which provides for liability for laundering of criminally obtained money and other property generally, allows for a proper adjudication of cases of money laundering committed through the use of cryptocurrency, and needs to be clarified only in terms of the possibility of recognizing the latter as the subject of money laundering. It is also necessary to develop a coherent methodology for investigating money laundering via cryptocurrency. The agenda of national regulatory authorities should include development (for some) and improvement (for others) of an effective system of state financial monitoring of service providers related to the circulation of virtual assets. This is not an easy task, but we express confidence that it needs to and can be done.

Given the complex nature of money laundering as a negative social phenomenon, which is extensively studied not only in legal but also in economic scholarship, the criminal law theory should employ the narrow legal definition of the relevant concept. In such aspect, legalization of the proceeds of crime should be understood as actions with property obtained as a result of a predicate offense aimed at making it look like property of legal origin for further use in economic or other legal activities. The proposed definition makes it possible to distinguish laundering from other types of circulation of property of criminal origin.

With the world's cryptocurrency market being valued at around $1 trillion, money launderers are focusing on its obvious advantages (such as speed of transactions, their volume and anonymity) when using various financial schemes to hide and launder assets. This poses a direct threat for national markets and financial systems. Despite analytical reports and proposed measures, including

various law enforcement initiatives, such emerging type of criminal activity has been steadily increasing both in numbers and geographical locations, which we have illustrated based on several high-profile cases. Such cases become even more complicated, since criminals use the best tools available to the two worlds – the digital (virtual) and the real one. Thus, a significant number of legislative and law enforcement measures on combatting crypto money laundering schemes should emerge in the near future. In this important battle, the world of law and justice has to prevail.

REFERENCES

18 U.S. Code § 1956 - Laundering of monetary instruments. Available at: https://www.law.cornell.edu/uscode/text/18/1956

2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking. *Chainalysis.* Available at: https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/.

Sanction Scanner (2023). Al Capone: The One Who Gives Us The Term 'Money Laundering'. Available at: https://sanctionscanner.com/blog/al-capone-the-one-who-gives-us-the-term-money-laundering-348#:~:text=Al%20Capone%20is%20also%20known,buying%20laundries%20in%20cash%20invisible.

Berest, M. (2023). NABU Detectives and Analysts Mastered the Crystal Blockchain: Details from the Member of Parliament. Available at: https://meta.ua/uk/news/tech/97956-detektivi-i-analitiki-nabu-opanuvali-crystal-blockchain-detali-vid-nardepa/.

Carillo, L. (2024). Brazil Arrests Man Suspected of Laundering Nearly US $2.66 Billion. *Organized Crime and Corruption Reporting Project.* Available at: https://www.occrp.org/en/daily/18355-brazil-arrests-man-suspected-of-laundering-nearly-us-2-66-billion.

Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022. (2022). Available at: https://www.chainalysis.com/blog/crypto-money-laundering-2022/.

Crystal School of Crypto Compliance and Investigations. (2023). Available at: https://crystalblockchain.com/training-and-certs/.

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843.

Dudorov, O. O. & Tertychenko, T. M. (2015). *Anti-laundering of "Dirty" Property: European Standards and Criminal Code of Ukraine*. Kyiv: Vaite.

Dumchikov, M, Horobets, N, Honcharuk, V & Dehtiar, R. (2022). Digital Currency as a Subject of Economic Criminal Offenses. *The Law, State and Telecommunications Review, 14 (1),* 20-30.

Dumchikov, M. (2022). Peculiarities of Counteracting the Legalization of Criminal Income with the Help of Virtual Assets in Cyberspace: Practical Dimension. *Law. State. Technology, 1,* 117-122.

Dyachkina, A. (2023). The Court Seized 1.5 Million Dollars of Crypto-Assets of the Ex-Head of the State Intelligence Service. Available at: https://www.epravda.com.ua/news/2023/11/30/707204/.

Dyntu V.A. & Mitrofanov A.A. (2017). Bitcoin in the System of Legalization of Proceeds of Crime. *Scientific works of the National University "Odesa Law Academy", 19,* 122-129.

EU Context of Anti-Money Laundering and Countering the Financing of Terrorism. (2023). *European Commission.* Available at: https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en?gclid=Cj0KCQiAsburBhCIARIsAExmsu4a0J5bgjDa6_nM4naIXlD97wt9N1ZA-OJ5qqIqw5RuLHenLaH4UdgaAmOTEALw_wcB.

Europol, 'From Suspicion to Action: Converting Financial Intelligence into Greater Operational Impact' (2017). Available at: https://www.europol.europa.eu/sites/default/files/documents/ql-01-17-932-en-c_pf_final.pdf.

Executive Order 14024 of April 15, 2021 "Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation". (2021). *Federal Register, 86 (73).* Available at: https://ofac.treasury.gov/media/57936/download?inline.

FATF (2020). Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.

FATF (2022). Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

Feliba, D. (2023). Cryptocurrency regulation comes into force in Brazil. *Fintech Nexus.* Available at: https://www.fintechnexus.com/cryptocurrency-regulation-comes-into-force-in-brazil/

Haffke, L., Fromberger, M. & Zimmermann, P. (2020). Cryptocurrencies and Anti-Money Laundering: the Shortcomings of the Fifth AML Directive (EU) and How to Address Them. *Journal of Bank Regulations, 21, 125-138*.

Hayes, A. (2023). Blockchain Facts: What is It, How It Works, and How It Can Be Used. *Investopedia.* Available at: https://www.investopedia.com/terms/b/blockchain.asp.

Honcharuk, V. L. (2021). Impact of Legalization (Laundering) of Proceeds Obtained Through Crime on the Economic Sphere of Ukraine in Modern Conditions. *Pravo.UA, 4,* 124-130.

Joining Forces: Public-private Partnerships vs. Financial Crime. (2023). *Forthline.* Available at: https://www.fourthline.com/resources/public-private-partnerships.

Kamensky, D. (2021). Globalization, COVID-19 Pandemic and White Collar Crime: A New Threatening Combination. *The Lawyer Quarterly, 4(11),* 625-640.

Kamensky, D. (2022). War and Law in Ukraine: Wheels of Justice Still Rotate. *The International Lawyer*, *55*(3), 541-550.

Koirala, B. (2021). 16 Advantages and Disadvantages of Cryptocurrency. Available at: https://honestproscons.com/advantages-and-disadvantages-of-cryptocurrency/.

Khomenko, V. (2023). 7 most important court cases regarding cryptocurrencies. Available at: URL: https://protocol.ua/ua/7_nayvaglivishih_sudovih_sprav_shchodo_kriptovalyut/.

Koshovyi, O. (2023). What is Wrong with the Law on Virtual Assets. *Mirror of the week. March 17, 2023* Available at: https://zn.ua/ukr/ECONOMICS/shcho-ne-tak-iz-zakonom-pro-virtualni-aktivi.html.

Money Laundering through Cryptocurrencies. (2024). *United Nations Office on Drugs and Crime.* Available at: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html.

Money Laundering. (2024). *United Nations Office on Drugs and Crime.* Available at: https://www.unodc.org/unodc/en/money-laundering/overview.html.

Ovcharenko, A.S. (2020). Virtual Assets as an Object of Financial Monitoring. *Bulletin Of Zaporizhzhya National University. Legal* Sciences, 3, 98-103.

Review of the Legislation on the Regulation of Virtual Assets in the Field of Combating Money Laundering and Terrorist Financing. (2022). Available at: https://fiu.gov.ua/assets/userfiles/310/%D0%A0%D1%96%D0%B7%D0%BD%D0%B5/VirtualAssets.pdf.

Richardson, I. & de Lucas Martin, I. (2021). *Investigation and Trial of Criminal Proceedings Regarding the Legalization (Laundering) of Funds.* Strasbourg-Kyiv: National School of Judges of Ukraine.

The Law of Ukraine from February 17, 2022 "On Digital Assets". (2022). Available at: https://zakon.rada.gov.ua/laws/show/2074-20#Text.

Townsend, J. (2001). Tax Crimes Materials. Houston: Townsend & Jones, L.L.P.

Treasury Designates Virtual Currency Money Launderer for Russian Elites and Cybercriminals. (2023). *U.S. Department of the Treasury.* Available at: https://home.treasury.gov/news/press-releases/jy1874.

U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws. (2023). Available at: https://home.treasury.gov/news/press-releases/jy1925.

Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals. (2019). *Congressional Research Service Report.* Available at: https://crsreports.congress.gov/product/pdf/R/R45664.

Zakharov, V.P. (2014). Legalization (laundering) of proceeds obtained through crime: theoretical and legal aspect. *Bulletin of the Lviv Polytechnic National University*. *Legal sciences, 801,* 180-186.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET