ESI Preprints **Not Peer-reviewed**

Cryptocurrency Abuse for the Purposes of Money Laundering and Terrorism Financing: Policies and Practical Aspects in the European Union and North Macedonia

Assoc. Prof. Dr. sc Ice Ilijevski
Prof. Dr. sc Goran Ilik
Faculty of Law, Kicevo
University "St. Kliment Ohridski", Bitola
Dr. sc Kire Babanoski
Independent researcher

Doi: 10.19044/esipreprint.3.2023.p23

Approved: 02 March 2023
Posted: 06 March 2023

Cite As:
Ilijevski I., Ilik G. & Babanoski K. (2023). *Cryptocurrency Abuse for the Purposes of Money Laundering and Terrorism Financing: Policies and Practical Aspects in the European Union and North Macedonia*. ESI Preprints.
https://doi.org/10.19044/esipreprint.3.2023.p23

Abstract

The number of countries that express concern for the danger of using cryptocurrencies for illegal activities among which are money laundering and terrorism financing is increasing. Cryptocurrencies are virtual assets created and managed through advanced computer encryption and operate on a decentralized network known as a blockchain. The key issue of concern and attention in the world is the anonymity and pseudonymity of cryptocurrencies, which prevents proper monitoring of transactions by state institutions and allows the completion of suspicious transactions outside the regulated systems. The paper provides an overview and presentation of the existing European legal framework and the measures and activities undertaken by the Republic of North Macedonia, harmonized with the European ones, in the fight against money laundering and terrorist financing in the crypto sector.

Keywords: Cryptocurrencies, money laundering, terrorism financing, European Union, Republic of North Macedonia

Introduction

Money laundering and terrorism financing have long been international issues that pose a serious threat to national and international financial systems and their institutions, as well as to the real economy and public safety. As the fight against money laundering and terrorism financing is a problem of global interest, it requires coordinated and cooperative action by a wide range of financial and security institutions nationally and internationally.

Money laundering and terrorism financing can often be closely linked, and their interaction is significant. The benefits of money laundering are enormous for criminals, and so are for terrorist groups and organizations. The techniques used for money laundering are similar or the same as those used to cover up the sources used to finance terrorism. It is important for terrorists to cover up the use of funds so that funding-related activities go undetected. Joint action according to previously established rules and standard procedures between the competent authorities and entities (financial institutions) that can be directly involved and used in the process of money laundering and terrorist financing enables greater caution and monitoring of all suspicious activities and of course timely action in direction of their prevention.

Through the process of detecting and preventing money laundering, the criminals and the terrorists are identified, as well as the activities they carry out through which they obtain funding. The application of intelligence and investigative techniques to track and detect their funding path can be effective in this process.

Methods

A qualitative approach will be used in this paper, using mainly analysis of the current legal framework and its novelties, such as policies, strategies and laws regulating the crypto-sector in the European Union and the Republic of North Macedonia. Furthermore, relevant academic publications in the field of crypto-sector opportunities and its relation to money laundering the terrorism financing will be also considered. The practicalities related to detecting frauds and abuses of cryptocurrencies and the existing preventive measures in North Macedonia will be presented, elaborated and reviewed through legal framework analysis and data obtained through free access to public information.

Results

Blockchain, bitcoin, crypto assets, virtual currencies... a whole new vocabulary describing innovative technology to swiftly transfer value around

the world. The fast-evolving blockchain and distributed ledger technologies have the potential to radically change the financial landscape (FATF).

Establishing a definition of cryptocurrencies is no easy task. Cryptocurrencies have become a "buzzword" to refer to a wide array of technological developments that utilize a technique better known as cryptography. In simple terms, cryptography is the technique of protecting information by transforming it (i.e. encrypting it) into an unreadable format that can only be deciphered (or decrypted) by someone who possesses a secret key. Cryptocurrencies are secured via this technique using an ingenious system of public and private digital keys (Houben & Snyers, 2018).

With the introduction of Bitcoin (James, 2018) (Bitcoin originated around the time of the global financial crisis, in 2008–09) a number of cryptocurrencies were developed and introduced on the market attracting considerable attention around the world (Fletcher et al., 2020). Cryptocurrency payments are characterized by a high degree of anonymity and the avoidance of monitoring and recording by law enforcement agencies. Precisely because of the complexity and anonymity, cryptocurrency transactions have a higher level of risk of money laundering and terrorism financing (Rysin, 2021).

There are many countries where cryptocurrencies are either unregulated or underregulated, effectively helping financial criminals conduct their activities unrestrained. The use of cryptocurrencies to make transactions has many advantages and disadvantages. In general, criminals are making use of these shortcomings for their fraudulent activities and profiteering. China's Payment & Clearing Association earlier said that cryptocurrencies "have increasingly become an important channel for cross-border money laundering" as they are global in nature, anonymous, convenient and fast to process. Some key factors (Tookitaki, 2021) that make cryptocurrencies attractive to money laundering are:

- Lack of regulation: Traditional financial channels are heavily regulated and legally protected across the globe. Meanwhile, cryptocurrencies are unregulated or loosely regulated in many countries and governments generally discourage their use of any kind. This lack of universal protection and regulation makes them attractive to criminals as effective means for cleaning illegal proceeds.
- Anonymity or pseudonymity: Many money laundering acts are made possible by the relative anonymity of cryptocurrency transactions. There are many wallet providers and crypto exchanges that offer services with little-to-no anti-money laundering (AML) or Know Your Customer (KYC) regulations in place.

– Payment option for a crime: Cryptocurrencies have already become a popular means of payment for criminal activities such as ransomware attacks and illegal online gambling.

Despite the promise of the open and transparent Blockchain ledger and the use of FinTech and RegTech software, there appear to still be ways of turning ill-gotten money in the real world, into clean cryptocurrency. The methods used still follow the traditional money laundering steps of (1) Placement; (2) Layering and (3) Integration. Some of these methods use the 'Dark Web' (Ratnatunga, 2021).

In addition to exchanges between virtual/fiat and virtual/virtual currencies and assets, the new FATF guidance captures entities involved in the transfer of virtual assets, the safekeeping of virtual assets, and the provision of financial services related to an issuer's offer or sale of a virtual asset within the definition of "virtual asset providers" (VASPs). This broadens the FATF's initial understanding of regulated entities and expands coverage to mixers and tumblers as well as initial coin offerings (ICOs) and other virtual asset investment technologies not captured in the 2015 guidance.

The FATF 2019 Guidance (Velkes, 2021) also defines virtual assets more broadly than its predecessor term, virtual currency, to include any "digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes". This new definition does not require recognition, meaning that a state-sponsored virtual currency would be subject to similar regulation. This indicates that FATF may be anticipating that countries will begin to either create their own or recognize other types of virtual assets. Most notably, however, the term includes any digital value that can be used for "investment purposes". This understanding greatly increases who is subject to mandatory registration as a VASP, sweeping many cryptocurrency investment-based services into the FATF regulatory framework and imposing a substantial regulatory burden on the industry. As FATF recommendations are not binding and allow members to implement national policy, the shift from virtual currency to a broader understanding of virtual assets may result in specific countries adopting different regulatory interpretations. Different national understandings of what a virtual asset is will lead to a disparate international AML regulatory framework, allowing money launderers to take advantage of differences across borders and evade law enforcement.

Discussion

European Strategic Framework against Money Laundering and Financing Terrorism

Ensuring the efficiency and consistency of the EU framework for combating money laundering and terrorist financing is of great importance. That is why the European Commission initiated and worked on a new legislative package that will implement the obligations in the Action Plan for a comprehensive policy of the Union for prevention of money laundering and terrorist financing, which was adopted by the European Commission on 7 May 2020.

On 20 July 2021, the European Commission presented an ambitious package of legislative proposals to strengthen EU anti-money laundering and anti-terrorist financing rules. The package also includes a proposal to create a new EU anti-money laundering body. This package is part of the commitment of the Commission for the Protection of EU Citizens and the EU financial system against money laundering and terrorist financing. The purpose of this package is to improve the detection of suspicious transactions and activities and to fill the gaps that criminals use to launder illegal income or to finance terrorist activities through the financial system. As stated in the EU Security Strategy 2020-2025, strengthening the EU framework for combating money laundering and terrorist financing will also help protect Europeans from terrorism and organized crime.

These measures greatly improve the existing EU framework, taking into account the new challenges related to technological innovation. These include virtual currencies, more integrated single-market financial flows, and the global nature of terrorist organizations. These proposals will help to create a much more consistent framework to facilitate compliance for operators subject to anti-money laundering and anti-terrorist financing rules, especially for those active across the border. One of those legal proposals is in fact the revision of the Regulation on the transfer of funds from 2015 for monitoring the transfer of crypto funds (Regulation 2015/847 / EU).

Currently, only certain categories of crypto-service providers are included in the scope of EU anti-money laundering and anti-terrorist financing rules. The proposed reform would extend these rules to the entire crypto sector, obliging all service providers to act appropriately towards their clients. These changes will ensure full tracking of transfers of cryptocurrencies, such as Bitcoin, and enable the prevention and detection of their potential use for money laundering or terrorist financing. In addition, anonymous crypto wallets will be banned, fully enforcing EU anti-money laundering and anti-terrorist financing rules in the crypto sector.

The requirements of the new regulation apply to cryptocurrency service providers whenever their transactions, whether in sovereign currency

or cryptocurrency, include: (a) traditional wire transfer or (b) cryptocurrency transfer between crypto-funded service providers and other indebted entities (eg, between two crypto-funded service providers or between crypto-funded service providers and another obligated entity, such as a bank or other financial institution). For transactions involving cryptocurrency transfers, all cryptocurrency transfers are treated with the same requirements as for cross-border wire transfers, in accordance with FATF Interpretative Note to Recommendation 16, rather than for domestic wire transfers, given the risks associated with cryptocurrency activities and cryptocurrency service provider operations.

The founder's cryptocurrency provider must ensure that the cryptocurrency transfers are accompanied by the founder's name, the founder's account number, where such an account exists and is used to process the transaction, and the address of the founder, the number of the official identity document, the identification number of the client or the date and place of birth. The founder's cryptocurrency service provider must also ensure that cryptocurrency transfers are accompanied by the username and user account number where such an account exists and is used to process the transaction.

The user's cryptocurrency service provider must implement effective procedures to determine whether founder information is included or followed in the cryptocurrency transfer. The user's cryptocurrency service provider must also carry out effective procedures, including, where appropriate, e-mail monitoring or real-time monitoring to determine whether the required information about the founder or user is missing.

The Crypto Sector in North Macedonia – Legal Framework

In the last few years in the Republic of North Macedonia, there is a pronounced entry of cryptocurrencies on the Macedonian market, and they are increasingly traded on world stock exchanges by Macedonian citizens. Globally, there are over 7,000 virtual assets traded on over 400 exchange offices. The identification of the types of virtual assets traded by domestic citizens is a particularly big challenge, especially since there are no legal competencies and authorities of a state institution for such checks and records. To illustrate, on the ranking list for the world index of adoption of cryptocurrencies for 2021 (Chainalysis, 2021), North Macedonia is ranked 123rd out of 157 countries, and in 2020 (Chainalysis, 2020) it is ranked 102nd out of 154 countries in the world. In addition to this, Article 114 of the old Law on Prevention of Money Laundering and Terrorism Financing stipulates that “the data, information and documentation collected, analyzed, processed and submitted by the Office under this Law are classified for which an appropriate degree of classification has been determined following

the regulations on classified information", and even if it has such information, the Financial Intelligence Unit may not share it publicly.

According to the information on the website of the National Bank of the Republic of North Macedonia (www.nbrm.mk), there is no generally accepted definition of cryptocurrencies in the country, and the current legal framework does not recognize the term "crypto-asset". Cryptocurrencies are considered as a specific type of intangible asset, based on certain technologies, which is not issued, nor its value is guaranteed by a central bank, it is not money, and the supply of these assets does not depend on the needs of the economy or the monetary system. The cryptocurrencies are in digital format and can be easily transferred online from any smart device. The crypto-funds are not a legal asset for payment in the Republic of North Macedonia, ie it is not allowed to pay with crypto-funds. The National Bank of the Republic of North Macedonia has no authority to regulate the creation, holding or trading, nor a supervisory role regarding crypto assets.

A working group has been established within the Ministry of Finance to prepare a report on the current situation, and plan and propose measures for the regulation of virtual assets and service providers for the exchange of virtual assets. Several solutions were proposed to be implemented in the new Law on Prevention of Money Laundering and Financing of Terrorism. For the first time, it defines virtual assets as follows: "digital securities or rights that can be stored, traded or transmitted electronically using record distribution technology or any similar technology and can be used for exchange or investment purposes". Virtual assets do not include digital records of fiat currencies or money within the meaning of the law which are legal tender, securities and other financial assets in accordance with the law. Whereas as a provider of services related to virtual assets is envisaged any natural or legal person whose business and professional activity consists in performing one or more activities or in providing one or more services related to virtual assets for or on behalf of another physical or a legal entity.

To offer protection against the misuse of virtual funds for money laundering and terrorism financing, the draft law covers: Services or activities related to virtual assets; Storage and administration of virtual assets or instruments that enable control over virtual assets; Organization of a virtual asset trading platform; Transfer of virtual assets; Execution of virtual asset orders on behalf of third parties; Participation and provision of services related to the offer of the issuer and/or sale of virtual assets; Virtual asset portfolio management; Receiving and transmitting orders for virtual assets; Virtual Asset Publisher; Public offering of virtual assets; Hosted and unhosted electronic wallet for virtual assets; Cryptomat, etc.

The most important part of the draft law (Macedonian Banking Association) is the provision where the providers of services related to

virtual assets are obliged in a transaction related to virtual assets with a value of EUR 1,000 or more according to the exchange rate of the National Bank of the Republic of North Macedonia on the day of the transaction in which another provider of services related to virtual assets participates are obliged to provide data on the ordering party and the recipient of the transaction (name and surname, title, address of the hosted or unhosted electronic wallet for virtual assets, etc.). Thereby, it is prohibited to provide services related to virtual assets that directly or indirectly enable the concealment of the identity of the client as well as performing transactions with such virtual assets. Also, a special provision prohibits financial institutions and virtual service providers from establishing or continuing a business relationship with Shell bank and starting or continuing a correspondent business relationship with a bank that they know allows opening and working with Shell bank accounts.

By introducing provisions for virtual assets/currencies in this draft law, without primarily creating and adopting legislation for this activity and for the conditions to be met by the providers of such services, there will be dangers of causing great uncertainty in the overall operation of financial institutions and would especially create confusion among residents when trying to conduct this type of transaction. Given that, it is necessary to specify which institution will be responsible for adopting bylaws in the field of providing services related to virtual assets.

The Financial Intelligence Unit, as the coordinator of a working group that includes representatives of the NBRNM, the Securities and Exchange Commission, the Public Revenue Office, the Financial Police, the Ministry of Finance and the Ministry of Information Society and Administration, has prepared an analysis with the involvement of the banking sector about the risks associated with money laundering and terrorist financing in connection with virtual assets and service providers which is currently an internal document.[1]

After the adoption of the Law by the Assembly of RNM, the Financial Intelligence Unit is a supervisory body on providers of services related to virtual assets, but only in terms of obligations arising from this law, ie in the implementation of measures and actions to prevent money laundering and terrorist financing. Investment aspects such as investor

[1] The information was received from the Financial Intelligence Unit through a submitted Request for free access to public information (submitted electronically on 26.12.2021, received a response on 28.12.2021)

protection and conditions under which virtual assets, insurance, consumer protection, etc. can be issued are aspects outside the scope of the law.

Conclusion

The era of globalization, openness and interaction between the financial flows of countries opens many risks and threats. Money laundering and terrorist financing are among those risks that for the security of countries, the region and the world must be detected and prevented on time. The fight against them in this era of global trade, services and transactions must be conducted at the international level, and for that purpose to build international cooperation between law enforcement agencies to ensure an adequate response.

Given that cryptocurrencies are already a reality and are used in cyberspace, but they pose a high risk of money laundering and terrorist financing, countries must adapt to such new conditions. Namely, control and supervision must be exercised over the providers of services related to cryptocurrencies, for example, first of all by establishing, maintaining and keeping a register of these persons. The National Unit for Financial Intelligence, specifically the Financial Intelligence Unit in the Republic of North Macedonia must have access to information related to the transfer of these cryptocurrencies, which it should receive from the providers of services related to such funds.

The banks are obliged to comply with the relevant requirements related to the foreign exchange regime, as well as the regulations related to the prevention of money laundering and terrorist financing. Due to the risk of money laundering and terrorist financing, the risk of temporary or complete blocking of certain platforms and freezing of clients' digital wallets increases, as a result of measures taken by the authorities to prevent money laundering and terrorist financing or the competent authorities for financial crime investigation. Financial institutions may also refuse to conduct cryptocurrency-related payment transactions if they believe that such transactions expose them or their clients to a high level of risk of money laundering or terrorist financing.

Given the absence of appropriate special legislation, the country should follow the European trends and recommendations of international financial institutions and establish certain rules that in the future would be translated into appropriate relevant legal solutions.

References:

1. Chainalysis (2020). *The 2020 Geography of Cryptocurrency Report Analysis of Geographic Trends in Cryptocurrency Adoption, Usage, and Regulation*. https://ag-pssg-sharedservices-

ex.objectstore.gov.bc.ca/ag-pssg-cc-exh-prod-bkt-ex/258%20-%20002%20Appendix%20B%20-%202020-Geography-of-Crypto%201.pdf

2. Chainalysis (2021). *The 2021 Geography of Cryptocurrency Report: Analysis of Geographic Trends in Cryptocurrency Adoption and Usage*. https://go.chainalysis.com/rs/503-FAP-074/images/Geography-of-Cryptocurrency-2021.pdf
3. FATF. Easy Guide to FATF Standards and Methodology. Virtual Asssets: What, When, How? https://www.fatf-gafi.org/media/fatf/documents/bulletin/FATF-Booklet_VA.pdf
4. Fletcher Emily, James Larkin Charles, Corbet Shaen. (2020). Cryptocurrency Regulation: Countering Money Laundering and Terrorist Financing. *SSRN Electronic Journal*.
5. Harold James. (2018). Throughout time, new currency has been associated with mystical qualities, and Bitcoin is no exception. *Finance & Development.* 55:2.
6. Houben Robby, Snyers Alexander. (2018). *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. European Parliament. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf
7. Law on Prevention of Money Laundering and Financing of Terrorism ("Official Gazette of the Republic of North Macedonia" No. 151/2022)
8. Law on Prevention of Money Laundering and Financing of Terrorism ("Official Gazette of the Republic of Macedonia" No. 120/2018 and "Official Gazette of the Republic of North Macedonia" No. 275/2019 and 317/2020)
9. Macedonian Banking Association, Comments and Questions on the Draft Law on Prevention of Money Laundering and Terrorist Financing, https://ener.gov.mk/files/Comment/142_%D0%9A%D0%BE%D0%BC%D0%B5%D0%BD%D1%82%D0%B0%D1%80%D0%B8_%D0%B8_%D0%BF%D1%80%D0%B0%D1%88%D0%B0%D1%9A%D0%B0_%D0%BF%D0%BE_%D0%9D%D0%B0%D1%86%D1%80%D1%82_%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%D0%BE%D1%82_%D0%B7%D0%B0_%D1%81%D0%BF%D1%80%D0%B5%D1%87%D1%83%D0%B2%D0%B0%D1%9A%D0%B51779122227.pdf
10. Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) COM/2021/422 final, https://eur-

lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0422
11. NBRM. Questions and Answers for the Crypto-Assets, https://www.nbrm.mk/prashanja-i-odgovori-za-kripto-sredstvata.nspx
12. Ratnatunga Janek. (2021). Money Laundering: Fiat Currency vs Cryptocurrency. *Journal of Applied Management Accounting Research*. 19:1.
13. Rysin Vitali. (2021). Vulnerability of virtual assets to illicit financial flows. *Economics, Entrepreneurship, Management*. 8:1.
14. Tookitaki (2021). *The Rise in Cryptocurrency Money Laundering Cases in 2021*. https://www.tookitaki.ai/news-views/the-rise-in-cryptocurrency-money-laundering-cases-in-2021/
15. Velkes Gabrielle Chasin. (2021). International Anti-Money Laundering Regulation of Virtual Currencies and Assets. *Journal of International Law & Politics*. 52:875. https://www.nyujilp.org/wp-content/uploads/2020/10/NYI304.pdf