RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
August 3-4, 2023

DOI:10.5281/zenodo.8310135

Considerations on Combating Money Laundry in the Field of Crypto-Assets, at European Union Level

Carmina-Elena Tolbaru

Lecturer PhD, The National University of Science and Technology POLITEHNICA Bucharest, Pitesti University Center, Romania, carmina.tolbaru@gmail.com

ABSTRACT: Money laundry is a boosting phenomenon worldwide, affecting multiple domains of social life, and we need sustainable efforts to hinder the actions committed by offenders to hide the profits obtained from their offences. The complexity and magnitude of this phenomenon taking place at present is explained within the context of growth of technology, which opens new horizons concerning offence-related opportunities. Thus, offences such as tax evasion, financing terrorist organisations, drug trafficking, corruption, frauds, as well as any other illegal financial activities, are committed regarding the offence of money laundry, witnessing a form of organised cross-border criminality. Starting in 2021, the rate of illegal use of crypto currencies for the purpose of money laundry has registered a significant growth, which made the European Union establish a new regulation framework in the field of combating money laundry, extending the field of application of rules to crypto-assets transfers. This paper analyzes the growing global phenomenon of the use of crypto-assets for criminal purposes, examines the regulatory framework in the European Union, and provides practical recommendations that can help prevent and combat money laundering.

KEYWORDS: money laundry, offenders, organised crime, crypto-assets, European rules

Introduction

Practical reality shows us an innovative facet of the phenomenon of money laundry, in terms of adjustment of a contemporary strategy in matter of illegal verification of the field of crypto-assets, the Europol studies revealing the amplitude of criminal activities regarding the illicit use of crypto currencies. Although the crypto currencies represent a technical innovation, at present being an extensive means of payment, of investment and of transfer of funds, their use for a crime-related purpose has become a practice in the absence of an efficient regulation. Usually, the illegal use of crypto currencies is associated with money laundry, the offenders showing ingenuity and refinement, taking advantage of technological innovation. The main "quality" of crypto currencies that offenders exploit illegally is that they ensure the illegal and anonymous transfer of value. In considering the wide field of crypto-assets, ensuring a transparent and safe economic and financial environment is a serious concern at the European Union level, the Commission analysing the implications of the crypto-assets in the crime-related sector.

Clarifications regarding the field of crypto-assets

In the 2023/1114 (EU) Regulation on markets in crypto-assets, the rules refer to the notion of crypto-assets as being defined as digital representations of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology (OJ, L 150/40, 2023, 41). As an example, we mention the blockchain technology which stores transactions in blocks by knots linked together by cryptography (Mehedințu and Georgescu 2023, 9). Thus, blockchain should be understood as a database, like a decentralised public registry, situated outside the action area of a central authority or of a go-between, in which there is registered information about the transactions made within such blockchain (Bamakan, Motavali and Bondarti 2020, 2), thus ensuring the transparency and integrity of internet transactions. Therefore, the blockchain is a transaction database, based on cryptography, using specific mathematical algorithms in order to create and verify a data structure which increases continuously, as other data can be added constantly, without being

able to delete them. Blockchain represents a distributed ledger held by every crypto-asset owner and updated with every transaction (Radu 2022, 17). This means that the blockchain has transparency as a feature, meaning that any transaction made within a blockchain, regardless of the moment of taking place and of the passage of time, can be tracked, allowing the identification of suspect models and behaviours. However, the field of crypto-assets represents a true crime-related ground, both crypto currencies and the other types of crypto-assets facilitating the activities specific to money laundry.

Thus, crypto-assets aim at a wide range of digital values which use cryptography that we can classify into three main categories, with reference to the functions they fulfil (Zlati 2021, 21-26):

- Crypto-assets used mainly as exchange means – being used to purchase goods and services from natural persons or merchants that accept such virtual currency as counter value (bitcoin, ether, Litecoin etc.);
- Utilitarian or utility crypto-assets – token allowing holders the right to access a platform/application, to use a certain service, or to purchase goods or services under preferential conditions;
- Crypto-assets with investment purposes – being equivalent to stocks, bonds or derived agreements, because they promise the investor future financial benefits resulted from the mere ownership of the crypto-asset.

Therefore, the legal framework in the matter should cover all the crime-related activities made through crypto-assets, each of them having its own characteristics and implications, from a legal point of view (Ionescu and Chiperi 2022, 10-18).

Crypto-assets and their potential criminality

Generally, crypto-assets include features regarding scalability, in terms of the number of transactions that can be processed within a certain time frame, and at the same time by a certain degree of anonymity, in relation to the blockchain used and the typology of the digital wallet used (Zlati 2021, 21-26). In this context, the crypto-assets have generated an outbreak of criminality. In the category of crypto-assets, crypto currencies are the most widespread means of payment, of investment and of transfer of funds, thus holding the highest rate among the money laundry offences. This field was harnessed by offenders, who exploited it to the full, the crypto-assets being used more and more in the criminal activity, both as an object of the offence, and as its product (Covolo 2019, 6).

Practical reality shows that we face a serious technological phenomenon, which is growing through the massive use of crypto-assets, especially by cyber-offenders, and we wish to list a few illegal operations, in order to reveal their criminal potential. Activities that are deemed as such (Zlati 2022, 10-69):

- mining virtual currencies, by the clandestine use of the power of processing the information systems (cryptojacking);
- obtaining virtual currency by blackmail (ransomware);
- obtaining virtual currency by fraud;
- unauthorised transfer of virtual currency and other crypto-assets;
- restraining access to virtual currency;
- identity fraud as a means of misleading;
- forgery of virtual currency;
- embezzlement of virtual currency transferred by mistake to another public address from the blockchain;
- money laundry – in terms of virtual currency, as well as other crypto-assets.

Money laundry has always existed and has covered different criminal forms, but globalisation, besides its undeniable benefits, has been the main indicator of growth of

criminality, especially the cross border one, the organised one. The problem at present and in this context is to regulate a legal framework that would control the abusive use of crypto-assets, without jeopardizing the evolution of the digital era. Undoubtedly, crypto currencies are the main target for the offenders. On top, there are indeed the cybercrimes, such as hacking, ransomware or cryptojacking, which raise real concerns in the field of cyber security, but we have to understand that money laundry is committed in relation to many offences from the organised crime sector, such as tax evasion, financing terrorist organisations, drug trafficking, corruption, frauds, as well as any other illegal financial activities committed in connection with money laundry offences.

In such a context, the concept of cryptographic criminality arises, concept used in connection with crypto-assets, the main risk in using crypto-assets being money laundry. Such a risk occurs as being generated by the fact that they allow transfers of assets, some of them pseudo-anonimous (bitcoin), some other anonymous (monero), outside central entity of control. There is a series of advantages of using crypto-assets for money laundry purposes (Puertas 2019, 25-27):

- hiding a cryptographic key is performed much easier than in the case of using cash;
- it assures a faster and safer way regarding the transfer of the value across borders;
- crypto-assets represent a good instrument for illegal investments;
- cryptographic wallets are outside the bank account files or other similar accounts.

In practice, when using crypto-assets, there is a series of behaviours and transactions that can raise suspicions, in identifying the suspect activities being able to apply specific identification principles and methods (Mehedințu and Georgescu 2023, 16):

- monitoring transactions – analyse the volume and frequency of transactions, of their value, and the participants involved;
- getting to know the clientele (know your client) – i.e., obtaining information regarding the identity of clients, purpose of transactions and source of the funds involved;
- analysing the transactions of a client by reference to his/her usual transaction profile - they analyse, by comparison, all the characteristics of the transactions and the previous behaviour of the client;
- collaboration and exchange of information between the reporting entities and the regulatory authorities – reporting the suspect transactions and sharing the relevant data.

The organisations specialised in fighting money laundry in the field of crypto-assets admit the challenges they are subjected to, by the difficulties they face in pursuing illegal activities, which should be constantly adapted to the *modus operandi* of digital offenders. The rapid evolution of technology imposes an adjustment of the suspicion indicators used to identify the behaviours that can be associated with illegal activities (Mehedințu and Georgescu 2023, 17):

- high-value transactions – which indicate the suspicion of existence of some illegal activities or the intention to hide illicit funds;
- transactions which involve frequent and rapid transfers of crypto-assets – which may indicate the attempt to hide the origin and destination of funds;
- frequent use of crypto tumblers – which allow the mix of crypto-assets by combining and mixing multiple transactions, which makes it difficult to identify the origin of funds;
- transfers towards unknown or suspect addresses – these being associated with illegal activities, such as dark web or ransomware;
- transactions towards states with weak or inexistent jurisdictions – the illicit funds being outside the regulation area.

The Europol studies has registered an increased growth of usage of cryptocurrencies in the money laundry schemes, showing that all criminal profiles are laundered with the help of crypto currencies (Europol 2021, 11). For offenders, cryptocurrencies are a means of payment for the purchase of illegal goods and services, such as drugs or materials of sexual abuse on

children, especially on darkweb-type markets. The phenomenon itself shows two types of entities and chain entities:

- the use of intermediary services and wallets (self-wallets, mixers, dark-net markets, and any other services, both licit and illicit. Such services are used by offenders to hold funds temporarily, to hide fund movements or to exchange assets;
- the fiat off-ramps – refer to services which allow the exchange of cryptocurrencies for fiat currency, this being the most important component in the process of money laundry and at the same time, a real threat for the entire crypto industry, from the perspective of illicit exchanges taking place on decentralised exchange platforms.

Enhancement of the European Union efforts in fighting against money laundry and financing terrorism

The concern for prevention of and fight against money laundry is a priority for all states of the world. According to the studies performed by Europol, in absence of legal regulation, the use of crypto-assets in criminal purposes has increased, being generated naturally by the significant growth of the use of crypto-assets amongst population (Europol 2021, p. 4). The phenomenon is spreading out of control, not being able to really be scaled, in terms of the characteristics regarding the anonymity of crypto-assets, which makes the fight against the abusive use of crypto-assets be one of the main priorities at European Union level. An important step in this regard is represented by the new rules targeting the crypto-assets markets and the transfer of funds, for a better financial transparency concerning the exchanges of crypto-assets. The necessity to solve this problematic issue occurs in the context where some exchange platforms do not allow the verification of the identity of users and of the transactions made by them, not being equipped with reporting procedures. From here, the necessity to implement some mechanisms of identification of users, of reporting the transactions made and of verifying them (Hegheș 2023, 41-42).

Within the context of fighting against money laundry with the help of crypto-assets, the Council of the European Union takes a stand for the measures that should be imposed in the crypto industry, by adopting new regulations to ensure the traceability of the crypto-asset transfers. In this field, the legislative proposals had as a starting point the fight against money laundry and financing terrorism, by the Directive (EU) 2015/849 on the prevention of use of the financial system for the purpose of money laundry or terrorist financing, document that has suffered significant amendments.

The reform of the European legal framework is based mainly on the obligation of crypto-assets service providers to collect ant to submit information regarding the initiator and the beneficiary of the transfers of crypto-assets made, so that suspect transactions may be identified and blocked. The assurance of the financial transparency concerning the exchanges of crypto-assets at the European Union level has in view the introduction of some ”travel rules” that should meet the requirements of the International Financial Action Task Force (FATF), a supervision body at world level in the field of money laundry and terrorist financing. Recently, they have published two extremely relevant regulations in the area of combating money laundry in the field of crypto-assets, i.e., (UE) Regulation 2023/1113 on the transfer of funds and (UE) Regulation 2023/1114 on markets in crypto-assets, in order to reduce the anonymity criteria.

Largely, (UE) Regulation 2023/1113 comes to complement the enforcement of FATF recommendations at world level, regarding the risks of money laundry and terrorist financing when virtual transfers or assets are transferred. An adjustment of the new regulation to the typologies of crypto criminality refers to the crypto ATMs which allow the users to make crypto-asset transfers towards an address for crypto-assets, by depositing of cash, often without any form of identification and verification of clients. By the anonymity offered by such ATMs in the performance of the crypto-assets transfers, by the fact that they offer the

possibility to operate with cash of unknown origin, they represent an ideal instrument for illicit activities, mainly in money laundry and terrorist financing. Therefore, the crypto-assets transfers related to crypto ATMs fall under the new regulation.

In considering the chain of payments and of crypto-assets transfers, the providers of payment services have the obligation to collect information regarding the payer and the beneficiary of the payment, and the providers of crypto-assets services have the obligation to make sure that the crypto-assets transfers are accompanied by information regarding the initiator and the beneficiary. In this context, it is imposed the obligation to check the accuracy of the information regarding the payer or the beneficiary of the payment in case of the transfers of funds exceeding the amount of EUR 1,000. The international cooperation within FATF involve high standards in the field of money laundry and terrorist financing, in this context having the answer of the European Union, by establishing a solid framework, by extending the field of application of the already existing rules to the crypto-assets transfers. Thus, the provisions of (UE) Regulation 2023/1114 on markets in crypto-assets target a wider range of providers of crypto-asset services than the ones the (EU) Directive 2015/849 used to refer to in the first instance, the obligations targeting both traditional institutions from the financial sector, and at the same time the new cryptographic actors, too, including the ones providing services related to crypto-assets within the European Union. By this regulation, the Member States have the obligation to implement into their legislation the new legal framework, applicable in 2024.

Conclusions

The technological advancement and the adjustment of criminal typologies to the dynamics of market digitalisation, is for offenders a breeding ground to exploit for criminal purpose, which implies strategic intervention on behalf of the regulatory authorities. The threats are bigger and bigger towards the economy and the financial integrity of any state, and the amplitude of the cases regarding money laundry by use of crypto-assets has become worrisome, especially since they enjoy covering worldwide. The unique characteristics of crypto-assets make them extremely vulnerable and, at the same time, attractive to be used for criminal purposes, this cryptographic creation generating typologies specific to money laundry. The biggest challenge lies in the anonymity of the ”crypto-creator”, the virtual asset transfers allowing themselves the anonymity, and also in the fact that cryptographic technology allows the rapid performance of transactions, the big money laundry schemes including thousands of transfer at a low cost. It is in the best interest to be aware of the cross-border aspect of this type of criminality, especially the risks presented by the abusive use of virtual assets for the purpose of money laundry and terrorist financing, which requires that the new standards imposed by the European Union be complied with and ensured worldwide.

References

Bamakan, S.M. Hoseeini, Motavali Amirhossein, and A. Babaei Bondarti. 2020. “A survey of blockchain consensus algorithms performance evaluation criteria.” *Expert Systems with Applications* 154(10):113385. DOI: 10.1016/j.eswa.2020.113385.

Covolo, Valentina. 2019. “The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti- Money Laundering Directive.” *University of Luxemburg Law Working Paper Series* 2019-015:1-24. delivery.php (ssrn.com).

Chainanalysis. 2022. Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022. Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022 - Chainalysis.

Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L 141, 5.06.2015, pp. 73-117).

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 (OJ L 156, 19.06.2018, pp. 43-74).

Europol. 2021. *Cryptocurrencies - Tracing the evolution of criminal finances*. *Europol Spotlight Report series*. Luxembourg: Publications Office of the European Union. Europol Spotlight - Cryptocurrencies - Tracing the evolution of criminal finances.pdf (europa.eu).

Hegheș, Nicoleta-Elena. 2023. "Biometric Identification: Opportunities and Challenges in the Digital World". *Proceedings of the 31st International RAIS Conference on Social Sciences and Humanities*, April 6-7: 40-44, Cambridge, MA: The Scientific Press. DOI:10.5281/zenodo.7900818.

Houben, Robby, and Alexander Snyers. 2018. *Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion*. Bussels: European Parlament. Cryptocurrencies and blockchain (europa.eu).

Ionescu, Adina-Mihaela, and Simona-Daniela Chiperi. 2022. "Token qualification by assessing whether they can be defined as security tokens or utility tokens." *Penalmente Relevant II:*10-18.1.pdf (penalmente.ro).

Mehedințu, Mihai, and Irina-Anca Georgescu. 2023. *Ghid privind indicatori de suspiciune și tipologii de spălare a banilor în domeniul cripto-activelor*. Bucharest: National Office for the Prevention and Combating of Money Laundering.

Puertas, Alexandra. 2019. *La lutte contre le blanchiment de capitaux a l'epreuve des crypto-actifs*. Paris: Universite Paris. Universite du Luxembourg - The EU Response to Criminal of Crytpocurrencies - 2019 Dec.pdf (theblockchaintest.com).

Radu, Bogdan. 2022. "Cryptocurrency – Nascent Regulation and Challenges for Romania". *Proceedings of the 26th International RAIS Conference on Social Sciences and Humanities*, February 27-28: 16-20, Cambridge, MA: The Scientific Press. DOI: 10.5281/zenodo.6414772.

Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (OJ L 150, 9.06.2023, pp, 1-39).

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 2023, 9.06.2023, pp. 40-205).

Zlati, George. 2021. "Blockchain technology, virtual currencies and criminal law." *Penalmente Relevant I:10-69.* 1.pdf (penalmente.ro).