ANTI-MONEY LAUNDERING STRATEGIES AND THE METAVERSE: NEW DANGERS AND OPPORTUNITIES[*]

Andrea R. Castaldo[**]

As we all know, money laundering consists of transferring illegally-obtained money through persons and bank accounts that are neither fictitious nor unlawful, so that its illicit origin cannot be identified[1].

This widespread criminal practice is not limited by national borders and must therefore be fought through shared strategies at the international level.

These prevention and repression standards are mainly set by the Financial Action Task Force on Money Laundering and the UN Global Programme against Money Laundering[2]. They consist in fostering customer identification processes, prohibiting banking secrecy, and keeping all bank transaction records for at least five years[3].

The most important money laundering prevention tools are: the acquisition and archiving of received data (the 'Data Layer'), constant monitoring of transactions (the 'Screening and Monitoring Layer'); reporting suspicious transactions (the 'Alert and Event Layer'),[4] and, lastly, analysis of the reports leading to a transaction being approved or blocked ('Operational Layer').

The precisely aim is to detect suspicious transactions, which the European Union consider to be those that 'give reasonable grounds to believe that money laundering or terrorist financing is being or has been committed or attempted, or that funds, regardless of their amount, are derived from criminal activity'.

Let us now see whether, and how, artificial intelligence, and in particular the Metaverse, can advance money laundering prevention, particularly in terms of client identification, tracing the origin of money and predicting people's investment initiatives.

[*] Testo della Relazione al "*6th International Forum on Persons Sought for Corruption and Asset Recovery*", Law School and College for Criminal Law Science of Beijing Normal University, Pechino (Cina), 10-11 dicembre 2022.

[**] Professore Ordinario di Diritto Penale, Dipartimento di Scienze Giuridiche presso l'Università degli Studi di Salerno.

[1] B.A. GARNER, H. CAMPBELL BLACK, *Black's Law Dictionary*, West, St. Paul (MN, USA), 2009, p. 1907.

[2] For a more detailed discussion, see, L. AI, *Anti-money laundering (AML) regulation and implementation in Chinese financial sectors: money-laundering vulnerabilities and the "rulebased but risk-oriented" AML approach*, in *University of Wollongong Thesis Collection*, 2012, p. 10 ff.

[3] J. HAN, Y. HUANG, S. LIU, K. TOWEY, *Artifcial intelligence for anti-money laundering: a review and extension*, in *Digital Finance*, 2, 2020, p. 214 ff.

[4] *Ibid*, p. 216 ff.

So far, artificial intelligence systems have supplemented compliance[5] processes, granting them greater automation and speed thanks to AI data retrieval and matching capability: this has facilitated customer identity verification, transaction monitoring, and automated information reporting.

The ability of artificial intelligence to automatically generate reports of suspicious activity is one of its main benefits in the field of anti-money laundering. Thanks to algorithms, Compliance officers can benefit from pre-filled suspicious transaction reports containing information about the transaction, its purpose, and the giver/recipient.

One of the current and issues, which will persist in the future, is how the advent of the metaverse will affect anti-money laundering strategies.

The term 'metaverse' is English, but it is made up of a Greek word, 'meta' ('μετά'), meaning 'beyond', and a Latin one, 'universe' (from 'universus'), meaning all natural phenomena seen as a whole. The definition 'beyond the universe' thus indicates a virtual universe, twin but alternative and parallel to the one in which we live.

The metaverse is normally a place to play, communicate, and learn, but it is also the setting to perform transactions using financial instruments, such as cryptocurrencies and non-tangible tokens (NFTs). Users can perform these activities by operating an avatar, i.e. a virtual identity that moves and acts in the Metaverse following human instructions. It appears that by 2026, 25% of us will spend at least one hour a day in this parallel, virtual dimension.[6]

The problem is that the creation of virtual identities that materially perform the physical transaction in the metaverse makes it more challenging to identify the physical person behind the avatar[7]. Furthermore, each avatar has a digital wallet for its investments, an autonomous virtual wallet for financial transactions in the metaverse[8]. This circumstance also makes it difficult to trace the origin of the invested capital as it is transformed from real to virtual currency before the transaction takes place in the metaverse. Lastly, the metaverse currently lacks clear and binding rules to prevent and fight crime. For example, the law to be applied and the authority that can intervene in the event of crimes committed in the metaverse have not been established[9].

[5] *Ibid*, p. 212.

[6] Press Release, *Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026*, 2022 (https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026).

[7] "Of most concern is the lack of Know Your Customer (KYC) checks performed on users", Napier Editorial Staff, *Battling financial crime in the metaverse*, in *Napier*, 2022 (https://www.napier.ai/post/financial-crime-metaverse-aml).

[8] Napier Editorial Staff, *Battling financial crime*, op. cit.

[9] "[…] more generally, a lack of consensus on what rules apply to the metaverse. The internet is not subject to any one central authority or regulatory framework, and it looks as if the metaverse is set to follow a similar direction", Napier Editorial Staff, *Battling financial crime*, op. cit.

All this means that the metaverse may facilitate crime, and it has been observed that 'the scope for money laundering has increased in line with the value of transactions taking place within these virtual environments [...] volumes of economic activity within the metaverse are not insignificant, with $500 million worth of activity across Decentral and Sandbox in 2021'[10].

Thus, while the metaverse may provide new opportunities for laundering illicit capital, if well managed and utilised, it might represent a 'new era' of prevention strategies.

For this to happen, the role of the blockchain as a 'digital footprint' of the transaction that took place in the metaverse is crucial.

Indeed, the blockchain provides all necessary information concerning a financial transaction performed in a given cryptocurrency. It is a tool designed to store digital information in order to create a secure and decentralised transaction[11].

Many of the projects created in the metaverse are based on blockchain technology with an important role assigned to NFTs: these, in fact, provide proof of ownership of a digital asset which, when recorded in the blockchain, makes it possible to certify the ownership and provenance of the asset. So, 'incorporating NFTs into the metaverse could enable and facilitate various activities related to the trading of digital products, as well as representing users with unique avatars, ultimately creating an economy within the metaverse'[12].

The blockchain also makes transactions (the so-called smart contracts) smarter, more autonomous, and faster. For example, if one wants to sell a product according to certain conditions, the blockchain makes it possible to automatically check that the potential buyer meets the requirements and, again automatically, completes the transaction once the check has been completed. From this point of view, the blockchain acts as a POS ('point of sale') which, having checked the availability of funds in the bank account associated with the credit card, automatically makes the payment. This form of contractual relationship was created in 1993 by Nick Szabo, referring to them as 'digital ATMs'. They are particularly advantageous in terms of speed and efficiency, as well as privacy since no third party comes between the buyer and seller. Lastly, these contracts are not subject to registration, transcription, or publication fees, so I'm sure they will become increasingly popular contractual instruments.

[10] *Ibid.*

[11] T.M. FERNÁNDEZ-CARAMÉS, P. FRAGA-LAMAS (eds), *Blockchain Potential in AI*, IntechOpen, 2021, p. 73 ff.; Q. YANG ET AL., *Fusing Blockchain and AI with Metaverse: A Survey*, in *IEEE Open Journal of the Computer Society*, 2022, p. 122 ff.; T.R. GADEKALLU ET AL., *Blockchain for the Metaverse: A Review*, 2022, p. 1 ff.

[12] TP&P Technology Editorial Staff, *Why Blockchain Is A Key Technology For The Metaverse?*, in *TP&P Technology*, 2022 (https://www.tpptechnology.com/en/blog/why-blockchain-is-a-key-technology-for-the-metaverse/).

All this calls for a radical change in anti-money laundering strategy, since a financial transaction can only be controlled through smart contracts once the transaction, which is performed automatically, has taken place. From this point of view, virtual platforms where smart contracts are performed will have to include compliance with anti-money laundering regulations among the conditions for concluding the financial transaction.

To summarise: on the one hand, blockchain reduces the anti-money laundering controls required for financial transactions. In fact, all transaction information is stored in the ledger and is guaranteed, in the sense that no one can alter or falsify the transaction data, and every transaction is recorded and visible to all parties with access to the blockchain. This ensures total transparency, and the metaverse is protected from illegal activities.

On the other hand, the speed at which transactions are carried out in the metaverse does not allow for timely monitoring of transactions that take place outside the certified and guaranteed circuits.

Indeed, it should be emphasised that the blockchain's traceability guarantees only apply to the exchange of assets such as NFTs and Bitcoin, which adhere to high transparency standards. Nevertheless, there are other cryptocurrencies which, despite having their own blockchain, cannot be traced (e.g. Monero)[13]. At the time of the transaction, these assets do not show the identities of the people making the transaction, indicating only their usernames, thus allowing them to evade traceability.

To make the preventive opportunities offered by the metaverse effective, it will therefore be necessary to identify common transparency and traceability standards for transactions within it, prohibiting the use of cryptocurrencies that do not guarantee them.

In conclusion, the blockchain can certainly represent an important tool to prevent money laundering, provided that all transactions carried out in the metaverse are carried out using assets whose blockchain allows them to be traced. To this end, it will be essential to have regulation at the supranational level, establishing the 'rules of the game' for all in the interest of security and privacy, with – at the same time – the possibility of reconstructing the paper-trail of each financial transaction.

[13] M. MOSER ET AL., *An Empirical Analysis of Traceability in the Monero Blockchain*, in *Proceedings on Privacy Enhancing Technologies*, 2018, p. 1 ff.