EXPLORING THE ROLE OF BLOCKCHAIN TECHNOLOGY IN ANTI-MONEY LAUNDERING

Evangelia Pappa, European University of Cyprus
Panagiotis Georgitseas, Panteion University of Social and Political Sciences
Georgios Tantis, Panteion University of Social and Political Sciences

ABSTRACT

In recent years, numerous financial institutions are investigating ways to improve the efficiency of handling data as they struggle to comply with new and impending regulations. By doing this, they hope to reduce the risks associated with improper data analysis and stop malicious activity from going unnoticed. One specific kind of technology that could supplement or even replace the existing AML/KYC processes is distributed ledger technology, or DLT which is more commonly known in the context of blockchain.

Keywords: Money laundering, Regulatory framework, European Directives, Blockchain, Blockchain Forensics.

INTRODUCTION

The core features of the contemporary globalized economy are centered on the intense interdependence of the financial system, through the large volume of international financial flows as well as the rapid advancement of technology. Characteristics that demonstrate the growth of organized and economic crime as well as the connections that exist between criminal organizations. Criminals seek refuge in opaque structures, with weak control mechanisms, in jurisdictions that provide secrecy, and in havens of anonymity and privacy.

Whenever a crime is committed and capital is accumulated, the criminal must consider how to conceal the evidence of his crime or how to spend their money without arousing suspicion (Mathers, 2004: 21). So, he launders money. Money laundering means taking money that comes from a criminal activity and using certain techniques in order to hide its illegal origin (Schott, 2006: I-3). The Financial Action Task Force (FATF) has defined "money laundering" as the processing of criminal proceeds to disguise their illegal origin in order to legitimize the ill-gotten gains of crime (OECD, 2009:11).

Money laundering is a transnational phenomenon that has been around for ages. Some researchers support the view that the term "money laundering" was first used from the practice of washing coins in casinos to ensure they did not spoil the white gloves of the casino ladies (Unger 2013), while others believe that it was dated back to the 1930s and was traced to Mafia ownership of laundries in the United States (Turner, 2011:2).

The United Nations Office on Drugs and Crime (UNODC) estimates that between 2 and 5% of global GDP is laundered each year. That's between EUR 715 billion and 1.87 trillion each year with less than 1% of this being caught. This reflects Eurojust's case statistics that show that money laundering cases accounted for almost 15% of all cases registered at the Agency between 2016 and 2021 (Eurojust, 2022).

Despite the efforts made in recent years by the majority of financial institutions to comply with the existing framework, the regulatory authorities have had to intervene in

Citation Information: Pappa E., Georgitseas P., Tantis G., (2024). Exploring the role of blockchain technology in anti-money laundering. *Journal of Legal, Ethical and Regulatory Issues*, 27(S3), 1-10.

several cases Blockchain is the technology that was originally developed to support the operation of cryptocurrency transactions and for this reason it was not initially given the importance it deserved. Over time, however, it proved to be a technology that, in addition to facilitating decentralized transactions, offers much more important functions such as transparency, security and data integrity. Due to these advantages, research on the use of blockchain has now expanded to various fields beyond payments such as: supply chain, healthcare, voting, property titles, copyright etc. In the area of regulatory compliance, blockchain has the potential to revolutionize the way regulatory bodies operate to date.

The article is structured in six sections. Following this introduction, the basic regulatory framework is presented. Section three describes the phases of money laundering and lists the methods used by criminals to "launder" ill-gotten funds. The section four presents an overview of the blockchain technology and the next section analyzes how blockchain technology could be beneficial in AML/KYC processes. The last section provides the concluding remarks.

THE BASIC REGULATORY FRAMEWORK

A key international effort to combat money laundering is the United Nations International Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, which was signed in Vienna in 1988, known as the "Vienna Convention". It was approved by the General Assembly on 20 December 1988 (decision 1988/8) and entered into force on 11 November 1990. The preamble of the Convention expresses the intense concern of the Parties from the growing illegal trafficking of narcotics and psychotropic substances and the interconnection with other organized criminal activities. The objective of the Convention is to promote close cooperation between the Parties, on the basis of bilateral, multilateral agreements or arrangements, and to take appropriate legal and administrative measures to suppress international criminal activities of illegal trafficking.

This was followed by the Council of Europe Convention, known as the "Strasbourg Convention" on the laundering, investigation, seizure and confiscation of the proceeds of crime and the financing of terrorism. It was approved by the Committee of Ministers of the Council of Europe in September 1990 and submitted for signature on November 8 of the same year. It entered into force on September 1, 1993. The convention sets out a set of rules that apply to criminal investigations that precede the issuing of a judgment and the execution of confiscation orders. A strong system of international cooperation is also being put in place to remove resources and proceeds from criminal activities.

The Strasbourg Convention was amended by the "Treaty of Warsaw", which was signed on May 16, 2005 and entered into force on May 1, 2008. It is expressly stated that "Each Contracting Party shall adopt the necessary legislative or other measures in order, in accordance with internal law to be established as crimes, when committed with intent: (a) the conversion or transfer of property with the knowledge of the fact that it derives from criminal activity or from an act of participation in criminal activity, with the aim of concealing or disguising its illegal origin or providing assistance to anyone involved in this activity, in order to avoid the legal consequences of their activity (Ackermann, 1992). For the purposes of the execution or application of paragraph 1 of this article: 1. it shall not matter whether the predicate offense is subject to the jurisdiction of the criminal courts of the Contracting Party, 2. it may be provided that the offenses referred to in that paragraph are not to the persons who committed the basic offense".

The second International Convention of the United Nations for the suppression of terrorism, known as "The Palermo Convention", is a legal basis for the promotion of the

Citation Information: Pappa E., Georgitseas P., Tantis G., (2024). Exploring the role of blockchain technology in anti-money laundering. *Journal of Legal, Ethical and Regulatory Issues*, 27(S3), 1-10.

cooperation of the member states to prevent and combat transnational organized crime. The Convention entered into force on 10 April, 2002. Article 2 defines an "organized criminal group" as a structured group of three or more persons that exists for a certain period of time and acts with the common purpose of committing one or more serious crimes, in order to directly or indirectly obtain financial or other material avail.

At European Union level, Directives have been enacted that adopt a holistic approach to anti-money laundering. More specifically, on June 10, 1991, the first Directive 91/308/EEC of the Council "on the prevention of the use of the financial system for the money laundering " was issued. With the adoption of the Directive, the member states undertook the obligation to establish the necessary legislative, regulatory and administrative measures to deal with the phenomenon before January 1, 1993. The content of the Directive was based on the United Nations Convention (1988) and on the recommendations of the Financial Action Task Force (hereinafter "FATF"), and also on the Council of Europe Convention (1990). The scope of the Directive was the prevention and control in order to safeguard the solvency and stability of the financial sector, including credit institutions and other financial institutions, in view of the completion of the Single Market.

On December 4, 2001, the second Directive 2001/97/EC of the European Parliament and of the Council "amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering" was issued. The scope of the revised directive includes the activities of "bureaux de change" and money remittance offices, investment companies in the securities sector, the verification of the identity of traders (and for ex distance transactions), keeping records and reporting suspicious transactions.

On October 26, 2005, the third Directive 2005/60/EC of the European Parliament and of the Council "on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing" was issued. The Directive is harmonized with the international framework formed following the revised recommendations of the FATF and other international bodies active in combating the relevant behaviors (UN, Council of Europe, Egmont Group). The Directive expands the range of basic offenses from the commission of which proceeds for legalization arise and specifies the due diligence measures for the customer.

On May 20, 2015, the fourth Directive 2015/849/EU was issued, which amended the previous one and provided for measures to combat new methods of money laundering with an emphasis on the real beneficiaries. It sets out an effective and comprehensive legal framework to tackle the raising of money or assets for terrorist purposes, requiring Member States to identify, understand and mitigate the risks related to money laundering and terrorist financing. Article 66 repeals Directives 2005/60/EC and 2006/70/EC with effect from June 26, 2017.

On May 30, 2018, the fifth Directive 2018/843/EU was issued, expanding its scope to deal with financial crime. Until then, cryptocurrencies, while convenient for conducting anonymous value transfers, escape the application of due diligence obligations. A solution to the problem is the extension of the scope of Directive 2015/849 to virtual currencies as well (recital 8 of Directive 2018/843). It becomes imperative to monitor the exchange of virtual currencies and fiat currencies (coins and paper money that are recognized as legal tender), as well as digital wallets. Therefore, exchange and custody service providers are defined as obligated persons, burdened with obligations to verify and verify the customer based on documents, verify the identity of the beneficial owner, update information, take reasonable measures, evaluate, collect information about the object and purpose of the business relationship and exercise continuous supervision. However, these obligations do not apply in the case that users use digital wallets, in which they store their private key at their own risk.

Citation Information: Pappa E., Georgitseas P., Tantis G., (2024). Exploring the role of blockchain technology in anti-money laundering. *Journal of Legal, Ethical and Regulatory Issues*, 27(S3), 1-10.

On October 23, 2018, the sixth Directive 2018/1673/EU "on combating money laundering by criminal law" was adopted by the European Parliament and the Council. According to this Directive, a "unified list of criminal acts" is created and twenty-two new offenses are introduced into the legislation, which the states must criminalize in their national legislations.

On May 31, 2023, Regulation (EU) 2023/1113 of the European Parliament and of the Council was issued on information accompanying transfers of monetary amounts and certain cryptocurrencies and on the amendment of Directive (EU) 2015/849 (recast), with the aim of combating money laundering and terrorist financing and strengthening the traceability of money transfers. The Regulation imposes information obligations on payment service providers, regarding the payer / sender and the recipient. Recasts Regulation (EU) 2015/847 on information accompanying money transfers, extending the information requirements that apply to electronic money transfers to cryptocurrencies.

Also noteworthy are the efforts of international organizations and agencies to draw up an anti-crime policy. A typical example is the FATF, the main international body activated to combat money laundering and terrorist financing. It was established by the Mission of the most economically powerful countries (G7) together with the President of the European Commission, in Paris in 1989, with the aim of developing international standards and policies against money laundering. In 1990 the newly established FATF issued the first standards including forty recommendations mainly on combating drug laundering, in 2001 it issued eight additional recommendations on the suppression of terrorist financing as a result of the terrorist attack on the twin towers and one recommendation on the cross-border transfer of funds. In 2003 they were revised, adding corruption and bribery to the basic money laundering offences, and in 2012, with the inclusion of the proliferation of weapons of mass destruction, they were enriched in terms of transparency requirements and became tougher in terms of corruption (Vassilantonopoulou, 2019).

In 2018, FATF updated its Standards to clarify the application of the FATF Standards to VA activities and Virtual Asset Service Providers (VASPs). To 2020 based on more than 100 cases studies, published a brief report analyzing the red flags indicators of money laundering and terrorist financing related to transactions, patterns, anonymity and geographical risks, indicators about senders or recipients and indicators in the source of funds or wealth.

MODELS AND TECHNIQUES OF MONEY LAUNDERING

In the section, the model of the three phases is presented in detail, which, although it is a simplified version of the multifaceted and complex process of money laundering, helps to understand the phenomenon. Next, the most common schemes adopted by the criminal are listed, depending on his capabilities and mode of action.

The modus operandi of criminals

In an attempt to determine the "modus operandi" of money laundering, various theoretical models have been developed that describe the fact that money laundering is not a single act but an interconnected process. The best known of these refer to the Zünd (1990) circular model, the teleological model, the Bernasconis' model (1988) and the American three-phase model (1989) adopted by the OECD. The latter, which is widely used, is depicted in Figure 1 and it is based on the description of the report of the Board of Governors of the Federal Reserve System (2002:7).

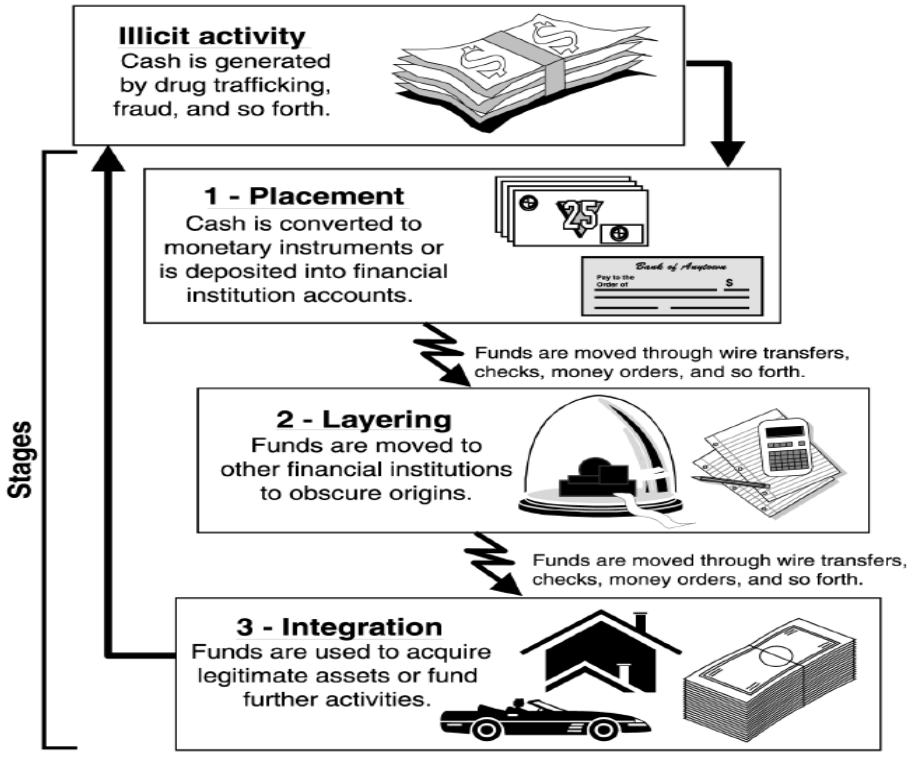
Citation Information: Pappa E., Georgitseas P., Tantis G., (2024). Exploring the role of blockchain technology in anti-money laundering. *Journal of Legal, Ethical and Regulatory Issues*, 27(S3), 1-10.

Placement is the initial phase of the money laundering process. The aim is to disguise the source of money and transform the illegal revenues, as a result of drug trafficking, human trafficking, extortion or other types of crime (‘dirty money’), into such a form that it makes difficult to trace its origin. Ways are being sought to 'wash' the ‘dirty money’ and place it in the legal economy (‘clean money’). Typical examples are bank deposits, real estate investments, the acquisition of shares, the purchase of precious metals, works of art, casino chips (Cox, 2014:16). The placement takes place in less well-regulated jurisdictions and the money is no longer liquid.

The next is the layering stage that is also referred to as 'agitation' or 'commingling' (Lilley, 2006:50). It is the separation of proceeds from the illicit source, creating layers of financial transactions to hide the route and provide anonymity (Bello, 2016:26). A critical point is the transfer of money within the same financial institution to other financial institutions, countries, currencies and even to other types of investments. Typical examples are buying and then selling an investment product, connecting payments to and from various personal and corporate accounts in different jurisdictions, participating in international trade transactions World Bank, 2009:265.

Finally, in the integration stage funds are put back into the financial system. The process refers to two phases, that of justification, that is, an apparently legal origin of the products of illegal activity is created, e.g. buying and selling real estate, buying legitimate businesses. And the investment phase where the proceeds of illegal activity are used for personal gain, purchase of high value items (jewelry, antiques, vehicles), purchase for personal use by check or credit card (CS, 2001:12). (Figure 1)

Figure 1
THE THREE-PHASE MODEL



Source: GAO (2002:7).

Citation Information: Pappa E., Georgitseas P., Tantis G., (2024). Exploring the role of blockchain technology in anti-money laundering. *Journal of Legal, Ethical and Regulatory Issues*, 27(S3), 1-10.

Money laundering schemes

During the stages of the legalization of illegal income, schemes are carried out to channel it into the legal economy, which in brief are (Richards, 1999: 67-70; Mathers, 2004: 152; Lilley, 2006:50; Schott, 2006: I-10; Alexander, 2016: 244; Madinger, 2012:243):

- *Currency Smuggling*: The simplest method is the physical transfer of cash to banking institutions that have lax control and strict secrecy. The transfer can be done either in suitcases, or in hiding places in trucks, by post, by private means of transport (vehicles, helicopters, aircraft, ships, etc.), on bowling balls, on children's toys.
- *Smurfing***:** Illegal capital is moved into the banking system through multiple and small transactions involving amounts below the threshold that would make a transaction suspicious. The amounts are then distributed to various accounts around the world, without appearing as suspicious transactions. For the implementation of the method, several partners are required, the so-called "smurfs", who will carry out the banking operations, which they then deliver to third parties, the intermediaries. The intermediaries will deposit the sums of money directly into the accounts of the perpetrators, in domestic or foreign banks.
- *Cuckoo Smurfing*: named after the cuckoo bird that lays its eggs in foreign nests for the host bird to raise its own. The choice of nest is not random, but the cuckoo tries to find a nest where its eggs will resemble those of the host, so that there is no chance of rejection. Respectively, criminals use the accounts of unsuspecting citizens in order to transfer their illegal capital across borders.
- *Hawala or underground banking*: a parallel banking system, used by individuals who want to avoid the banking system and paying taxes. The transfer is in cash from developing to developed jurisdictions. They operate behind front businesses (bakeries, car washes), making the process invisible to the authorities. The illegal money is transferred in cash, through an intermediary.
- *Jewelry Business*: The investment in luxury goods either for personal use or for resale. The nature the business involved in the buying and selling of these goods (diamonds, gold) is focused on secrecy and weak control.
- *Casino and gambling*: 'Lucky' winnings are difficult to define and pinpoint.
- *Exchange offices*: The money is converted into the national currency of the country to which it has been transferred and then deposited into domestic bank accounts and lastly transferred to the country of origin.
- *Safety Deposit Boxes*: The problem with safety deposit boxes is that no one knows their contents, and can be accessed by a third party who is declared in advance.
- *Payable Through Accounts*: specific bank accounts, opened in American banks by foreign banks to serve their customers. Customers manage to make transactions in American banks because only the foreign bank in America is visible.
- *Stock Products*: Bonds, Mutual Funds, Small Value Stocks, Penny Stocks, Options.
- *Bank lending*: With bank lending, the criminal will easily and quickly receive money in his bank account, which he will pay back in the form of loan installments. These loans are low-interest, or may be given at zero interest, by banks involved in the criminal network. Loans are given as collateral for the "customer's" deposits in Swiss banks.
- *Tax havens and offshore companies*: countries - states that have a special tax policy with low or no taxation for those foreign investors who establish companies there, transfer their funds or assets. In the second phase of money laundering (layering) and then at the integration stage, corporate vehicles play a vitally important role. This includes companies, trusts, foundations, non-governmental organizations.

Citation Information: Pappa E., Georgitseas P., Tantis G., (2024). Exploring the role of blockchain technology in anti-money laundering. *Journal of Legal, Ethical and Regulatory Issues*, 27(S3), 1-10.

AN OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Blockchain technology became widely known as the underlying technology of the Bitcoin network which was the first fully decentralized peer-to-peer payment system (Nakamoto, 2009). The main reason why this technology is considered the most revolutionary is that it introduced a specific way of organizing, storing and sharing data and information. In other words, it enables the validation of data and its permanent recording in distributed networks without the need for the intervention of a central authority or a trusted third party. Blockchain technology is often referred to as distributed ledger technology - DLT as a blockchain network is essentially a distributed database. The term distributed networks refers to networks that are not subject to any central authority. That means that each user (node) of the network is directly connected to the other nodes of the network and all users simultaneously have the same access to all the information recorded in the specific network.

Every transaction in a blockchain network is conducted peer-to-peer between users and appears throughout the network as encrypted information. Then the transaction is included within a block which contains data from a set of transactions. The block with the encrypted data is broadcasted to all the nodes (users) of the network and a certain percentage of nodes are required to validate it (Zhao et al, 2016). The validity of each block is determined after a consensus of the network nodes according to a predefined algorithmic validation method known as a "consensus mechanism". The term "consensus mechanism" refers to a set of rules for verifying and validating transactions, which are determined based on the network's computing protocol and which the network community must adhere to. At this point it is important to mention that each blockchain network can have its own validation rules, which justifies the existence of several different consensus mechanisms.

The above process of validation in a blockchain network is known as "mining", and the specialized users of the network, who validate the data, are the so-called miners (Niforos et.al, 2017). In order to create a block, miners generate a unique string of numbers and letters called a "hash" by running transactional data through a mathematical algorithm. The block is then updated with the hash value. To ensure that the data in a block can never be altered, a hash value is used. A small alteration to the data would result in a change in the hash value and the block being identified as fraudulent (Vasilantonopoulou, 2019). The data and information contained in each block is considered valid only after its validation process is completed. The block is then added to the chain of previously validated blocks and the information cannot be deleted or modified. In this way, a chain of blocks is created (blockchain) which are connected to each other using encryption techniques.

A blockchain network can be Public which means anyone can participate, it can be Private where access is only allowed to registered users, or it can be Consortium in the sense that it is partially centralized (Zheng, et.al, 2017; Jaag & Bach, 2017). An additional important distinction between the blockchain networks concerns the Permissionless blockchains that do not require authorization and therefore each user can read or register data in the blocks and the Permissioned blockchains that require authorization which means that specific rights are granted to predefined users.

An additional innovation brought by blockchain technology is the so-called "smart contracts". A smart contract is a computing protocol in which the terms of any agreement can be recorded in the form of computer code. When all terms and conditions recorded in a smart contract are met, then it is automatically executed on the blockchain without the intervention of intermediaries (Wright & De Filippi, 2015). In other words, smart contracts make it

Citation Information: Pappa E., Georgitseas P., Tantis G., (2024). Exploring the role of blockchain technology in anti-money laundering. *Journal of Legal, Ethical and Regulatory Issues*, 27(S3), 1-10.

possible to record in blocks not only data of financial transactions but also data of any scheduled order that has been agreed upon. In addition, smart contracts are automatically executed exactly as programmed, without the need for intermediaries or the ability to interrupt them.

From the above it is easy to understand that a blockchain network is essentially a distributed database i.e. a digital platform or a digital registry, which uses cryptographic methods to record, validate and store information, which cannot be hacked while it is available to all network participants in a secure and transparent way. (Wright and De Filippi 2015; Kakavand et.al, 2017) That is, it creates an environment of reliability and trust in data distribution without requiring the intervention of a trusted third party while at the same time provides the infrastructure to create, execute and store all kinds of data.

THE USE OF BLOCKCHAIN TECHNOLOGY FOR COMPLIANCE

The main benefit of using DLT technology to combat money laundering is data integrity. In order to register and store data in a blockchain network, is required the consensus of the network's participants that all information is accurate and true. This means that listing information about a customer such as their financial profile, transaction history, financial details and source of income is almost impossible to be false or the result of internal fraud. Furthermore, once the information is verified and recorded on the blockchain, it is almost impossible to hack or leak personal data since it is cryptographically hashed.

In addition, proper implementation of distributed ledger technology can significantly upgrade Know Your Customer (KYC) processes. In such a sense, all information regarding a customer's identity could be stored in a Private and Permissioned blockchain network that would be accessible to a country's banks, tax authorities and regulatory authorities. This means that all the above organizations and authorities will have simultaneous access to the same information and will be able to use it appropriately during the Customer due diligence (CDD) process. In addition, any change to the customer's details will be immediately visible and will be validated by all participating network operators. Based on the above, one realizes that technology can not only simplify the Know Your Customer (KYC) process and make it faster but can also make it more secure by eliminating cases of human error or internal fraud.

Let's suppose that a customer opens an account at Bank A after completing the standard onboarding process. If the same customer wants to open a new account in the Bank B, then the same process will have to be repeated. The solution offered by the DLT technology is that Bank A can share the customer's digital identity with Bank B removing the need for the customer to resubmit personal information, since the two banks participate in the same blockchain network. In this case, Bank B will save time and resources by receiving the information provided by Bank A, allowing for a simpler and faster onboarding process. Furthermore, every node has a record of the entire ledger, so any changes can be compared to their record to identify any unauthorized changes. Because of this specific feature of blockchain technology, DLT ledgers are entirely reliable. As a result, regulators could review records with confidence that the data they contained was accurate and dependable.

Finally, an AML/CFT program incorporating blockchain technology and smart contracts would have the capability to automatically enforce AML regulations, detect fraudulent activities, and combat money laundering through the utilization of built-in algorithms. By incorporating a set of conditions, such as the requirement for verified identification, this advanced technology has the capability to automatically prevent or raise an alert for any potentially suspicious or prohibited transactions. The implementation of such a system makes feasible to monitor and track all electronic transactions conducted through

Citation Information: Pappa E., Georgitseas P., Tantis G., (2024). Exploring the role of blockchain technology in anti-money laundering. *Journal of Legal, Ethical and Regulatory Issues*, 27(S3), 1-10.

designated financial establishments, eliminating the need for extensive manpower to inspect transactions and identify any potentially illicit behavior.

CONCLUSION

It is clear that blockchain technology provides a unique opportunity for financial institutions and regulatory authorities to effectively deal with or at least significantly minimize fraud and money laundering which has been on the rise in recent years. When KYC documentation was integrated into a private ledger and shared simultaneously among member banks there would be no need for each bank to conduct duplicate KYC due diligence on the same customer. Also, if regulators participate as node in a private blockchain, they could obtain reports of suspicious activity in real time. Finally, as blockchain technology preserves an uninterrupted audit trail of each transaction on the network. It becomes more challenging for money launderers to conceal their transfers by using several shell accounts.

The blockchain's potential is much greater than the implementations described above. Blockchain technology can play a fundamental role in improving regulatory reporting, identity management, due diligence, and transparency if regulators, financial institutions, and auditors, cooperate and harmonise their efforts. Concurrently, these advancements could make it increasingly challenging for illegal activity to go undetected.

CONTRIBUTIONS

The authors contribute independent work to the text. The first author contributes to the sections “ABSTRACT”, “INTRODUCTION”, “MODELS AND TECHNIQUES OF MONEY LAUNDERING” and “CONCLUSION”. The second author contributes to the sections “ABSTRACT”, “INTRODUCTION”, “AN OVERVIEW OF BLOCKCHAIN TECHNOLOGY”, “THE USE OF BLOCKCHAIN TECHNOLOGY FOR COMPLIANCE” and “CONCLUSION”. The third author contributes to the section “ABSTRACT”, ‘THE BASIC REGULATORY FRAMEWORK’ and “CONCLUSION”.

REFERENCES

Ackermann, J. B. (1992). Geldwäscherei–Money Laundering. Eine vergleichende Darstellung des Rechts und der Erscheinungsformen in den USA und der Schweiz, Zürich.

Alexander, R. C. H. (2016). Insider dealing and money laundering in the EU: law and regulation. Routledge.

Bello, A. U. (2017). Improving anti-money laundering compliance: Self-protecting theory and money laundering reporting officers.

Board of Governors of the Federal Reserve System. 2002. Report to Congress in Accordance with §356c of the USA Patriot Act. Washington, DC: Board of Governors of the Federal Reserve System.

Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.

Cox, D. (2014). Handbook of anti-money laundering. John Wiley & Sons.

CS (2001). A Model of Best Practice for Combating Money Laundering in the Financial Sector; Economic Paper 43, Commonwealth Secretariat.

Daskalakis N., Georgitseas P.,(2023). Fintech and Cryptoeconomy, Propobos Publications, Athens (In Greek)

Daskalakis, N., & Georgitseas, P. (2020). An introduction to cryptocurrencies: the crypto market ecosystem. Routledge.

Directive (EU) 2015/849 EC of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

Citation Information: Pappa E., Georgitseas P., Tantis G., (2024). Exploring the role of blockchain technology in anti-money laundering. *Journal of Legal, Ethical and Regulatory Issues*, 27(S3), 1-10.

Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law.

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.

Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

Eurojust (2022). Eurojust Report on Money Laundering. Criminal justice across borders.

GENERAL ACCOUNTING OFFICE WASHINGTON DC. (2002). MONEY LAUNDERING: Extent of Money Laundering through Credit Cards Is Unknown.

Jaag, C., & Bach, C. (2017). Blockchain technology and cryptocurrencies: Opportunities for postal financial services (pp. 205-221). Springer International Publishing.

Kakavand, H., Kost De Sevres, N., & Chilton, B. (2017). The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. Available at SSRN 2849251.

Lilley, P. (2003). Dirty dealing: the untold truth about global money laundering, international crime and terrorism. Kogan Page Publishers.

Madinger, J. (2011). Money laundering: A guide for criminal investigators. CRC Press.

Mathers, C. (2004). Crime school: Money laundering: True crime meets the world of business and finance. Firefly Books.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Niforos, Marina; Ramachandran, Vijaya; Rehermann, Thomas., (2017). Block Chain: Opportunities for Private Enterprises in Emerging Market. International Finance Corporation, Washington, D.C.. © International Finance Corporation. License: CC BY-NC-ND 3.0 IGO

OECD, (2009). Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors.

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.

Richards, J. R. (1998). Transnational criminal organizations, cybercrime, and money laundering: a handbook for law enforcement officers, auditors, and financial investigators. CRC press.

Schott, P. A. (2006). Reference guide to anti-money laundering and combating the financing of terrorism. World Bank Publications.

Turner, J. E. (2011). Money laundering prevention: Deterring, detecting, and resolving financial fraud.

Unger, B. (2013). Introduction. In B. Unger & D. van der Linde (Eds.), Research handbook on money laundering (pp. 3–18). Cheltenham: Edward Elgar Publishing.

Vasilantonopoulou, B. "Anti-criminal money laundering policy as latent economic governance". In S. Vidali, N. Koulouris, X., Papacharalambous (2019). Crimes of the powerful: Economic, organized crime and corruption. Athens: EAP Publications (In Greek).

Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. Available at SSRN 2580664.

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial innovation, 2, 1-7.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). Ieee.

Zünd A. (1990). Geldwäscherei: Motive-Forme-Abwehr, Der Schweizer Treuhunder.

Received: 02-Feb-2024, Manuscript No. JLERI-24-14593; **Editor assigned:** 03-Feb-2024, Pre QC No. JLERI-24-14593(PQ); **Reviewed:** 17-Feb-2024, QC No. JLERI-24-14593; **Revised:** 22-Feb-2024, Manuscript No. JLERI-24-14593(R); **Published:** 29-Feb-2024

Citation Information: Pappa E., Georgitseas P., Tantis G., (2024). Exploring the role of blockchain technology in anti-money laundering. *Journal of Legal, Ethical and Regulatory Issues*, 27(S3), 1-10.