فصلنامه پژوهش های نوین در علوم انسانی و حقوق شماره 1- دوره2- صفحات158-170
Journal of new Researches in Humanities and Law
ISSN 3060-6101

Money Laundering Using Privacy-Based Cryptocurrencies: Legal and Regulatory Challenges and Responses

Seyed Amir Mohammad Mirtavana

Abstract

Money laundering through privacy-based cryptocurrencies poses a serious challenge to financial supervision and the enforcement of anti-money laundering (AML) regulations at the national and international levels. These currencies, which use advanced technologies such as Ring Signatures and Zero-Knowledge Proofs to conceal the identity and financial transactions of users, have become a suitable platform for criminal activities and money laundering. The privacy-preserving capabilities of these currencies pose significant challenges in the enforcement of anti-money laundering laws, especially in a situation where regulatory authorities face serious limitations in tracing transactions. Money laundering through privacy-based cryptocurrencies is a complex legal and regulatory challenge that requires multifaceted responses from judicial, regulatory and supervisory authorities. Effective measures to combat this phenomenon should include the development and harmonization of international anti-money laundering laws, the use of advanced technologies to trace transactions, strengthening the accountability of exchanges and expanding international cooperation. Only by implementing these measures and more rigorous monitoring. Financial activities in the cryptocurrency space can effectively combat money laundering threats and ensure global economic security.

Domestic regulatory laws and protocols of different countries are interdependent. Only through stricter implementation of FATF guidelines, development of new blockchain analysis tools, and strengthening the responsibility of exchanges and platforms can money laundering in the cryptocurrency world be effectively combatted. Expanding international cooperation in the field of financial information exchange and judicial protocols can also help in monitoring and transparency in this area.

Keywords: Money Laundering, Cryptocurrency, Privacy, Coping methods

1.Introduction

In today 's modern world, digital currencies have become one of the main tools in financial transactions. This innovative technology has not only created new possibilities for carrying out financial transactions, but also , due to its special features , has become a complex and challenging tool in combating financial crimes such as money laundering . One of the most controversial and at the same time complex areas in this field are privacy - based cryptocurrencies.Currencies like Monero and Zcash , which use advanced technologies such as Ring Signatures and Zero - Knowledge Proofs to hide user identities and transaction details , provide financial criminals with a convenient opportunity to launder money . These features , along with the decentralized and global nature of digital currencies , have made monitoring financial activity a difficult task for law enforcement and regulatory agencies .

Money laundering through private digital currencies poses a serious challenge to international legal and regulatory frameworks . These currencies , especially in the context of decentralized blockchains , which are not easily transparent and traceable , allow criminals to move illicit funds and make it very difficult to trace them . In addition , the lack of harmonization of laws and the lack of effective cooperation between countries have become one of the biggest obstacles in combating this phenomenon .In this regard , the need to reform and update anti - money laundering (AML) and know - your - customer (KYC) laws , especially in relation to privacy - based digital currencies , is becoming more and more urgent .

This article is an analysis of the challenges and legal issues arising from money laundering through private cryptocurrencies . In this analysis , while examining the existing regulatory and legal challenges , various solutions will be proposed , such as strengthening international cooperation , employing new technologies for transaction tracking , and updating national and international laws . The goal is to provide a comprehensive picture of the current state of laws and regulations in this field and how to effectively deal with these threats in order to achieve positive results in the fight against money laundering in the digital currency space.

2.Features of Privacy - Based Cryptocurrencies

Privacy - based cryptocurrencies are specifically designed to keep users ' identities and the details of their financial transactions hidden from public view. Unlike Bitcoin and other digital currencies, whose transactions are recorded on a public ledger (blockchain) and the identities of some users can be traced through transaction analysis, privacy - based currencies use techniques such as Ring Signatures and Zero - Knowledge Proofs to hide the identities of the parties to the transaction and the transaction amount**.**

3.Challenges Arising from the Use of Privacy - Based Cryptocurrencies in Money Laundering

A. Anonymity and untraceability of transactions:

Privacy - based cryptocurrencies have the advantage of making it very difficult to trace and identify amounts , recipients , and senders of money . This is particularly attractive to economic criminals, as they can use this technology to easily transfer funds from their illegal activities and convert them into legitimate sources without being detected .

B. Challenges related to sovereignty and judicial competence:

Given the global nature of cryptocurrencies and their lack of geographic boundaries , there are governance issues regarding the monitoring and enforcement of transactions and money laundering activities . Many countries may have different laws regarding the use of digital currencies and the fight against money laundering , which reduces the possibility of synergy between countries in this area .

C. Lack of global regulatory standards:

There is still no comprehensive international supervisory framework to combat money laundering through privacy - based cryptocurrencies . International organizations such as The FATF (Financial Action Task Force) has attempted to develop guidelines for monitoring digital currency transactions , but these guidelines are still inadequate against the more sophisticated techniques employed by this type of cryptocurrencies .

3-1.Legal and ethical challenges in combating money laundering through digital currencies

A. The conflict between privacy and national security:

One of the major challenges in combating money laundering through privacy - based cryptocurrencies is the conflict between individuals ' right to privacy and the need to protect national security . While many proponents of digital currencies emphasize the need to protect individuals ' privacy , regulatory and judicial authorities They seek to increase transparency and reduce the use of these currencies in illegal activities . This conflict has become a legal issue in many countries, as some believe that surveillance measures may lead to violations of individual rights .

B. Different policies in different countries:

While some countries , such as the United States and the European Union , place a strong emphasis on monitoring and prosecuting money laundering in digital currencies , others have more flexible laws . This difference in policies and approaches adds to the problem of global coordination and may turn some countries into money laundering havens . As a result , A coordinated international legal framework to combat money laundering seems essential .

Legal Challenges in Combating Money Laundering in Privacy - Based Cryptocurrencies

3-2.Legal Challenges in Combating Money Laundering in Privacy - Based Cryptocurrencies

The fight against money laundering in the field of cryptocurrencies , especially those digital currencies that operate on the basis of privacy technologies , has created complex legal challenges . These challenges relate not only to technical and security aspects , but also to fundamental issues such as privacy . It also includes privacy , personal data protection , national sovereignty , and judicial competence . This section analyzes these challenges from a legal perspective .

A. Privacy rights and human rights:

One of the most fundamental legal challenges in combating money laundering in privacy - based cryptocurrencies is the conflict between privacy rights and the need for transparency in transactions . Human rights , in particular the principles related to privacy , are formally recognized in many countries in the form of international covenants and conventions . In this regard , Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) explicitly defend the right of individuals to privacy.

However , in the digital era , and especially in the field of cryptocurrencies , significant legal challenges arise , especially in the areas of financial supervision and the fight against financial crimes . The use of currencies such as Monero and Zcash , which are specifically designed to protect the identity of users and transaction details , becomes a fundamental issue in the violation or protection of privacy . In this context , a balance must be struck between the protection of privacy rights and the need for financial transparency , which is essential to prevent money laundering and ensure financial security .

B. Legal challenges to national sovereignty and judicial competence:

Money laundering using privacy - based cryptocurrencies poses serious challenges to national governance and jurisdiction . Digital currency transactions , which are typically conducted on decentralized and transnational blockchains , pose challenges in determining who is responsible for the money laundering . Which national institution is responsible for monitoring and prosecuting those transactions ? This lack of judicial transparency leads to problems in prosecuting criminals and enforcing court orders when transactions are transferred from one country to another .

From a legal perspective , the issue of jurisdiction in the area of money laundering in privacy - based digital currencies can cause disputes between countries . For example , if an individual uses privacy - based digital currencies in a country that has laws to track and monitor transactions (such as the United States or European Union countries) , while another country with weaker laws (such as some African countries) or Asia) , this can lead to challenges in enforcing laws and monitoring transactions . Lawmakers also face the challenge of whether to incorporate national sovereign rights into their laws or to adopt an international approach to combating money laundering .

C. Responsibility of cryptocurrency exchanges and financial service providers:

One of the key legal challenges in addressing money laundering in cryptocurrencies , especially privacy - based currencies , is the liability of exchanges and financial service providers . Under global anti - money laundering (AML) regulations , many countries have imposed requirements on digital currency exchanges to conduct rigorous and ongoing monitoring measures , including Know Your Customer (KYC) and Suspicious Activity Reporting (SAR) . This is while privacy - based digital currencies , due to features such as ring signatures and zero - knowledge proofs , are less transparent and difficult for exchanges to monitor .

The legal liability of exchange offices for the use of private currencies for money laundering is still not fully clarified in many countries . While some countries , such as the United States and European countries , require exchange offices to carry out detailed controls KYC and AML , in some other countries there are still no precise and transparent laws in this field . Therefore , Exchanges and financial service providers must face legal challenges related to the inability to accurately track and identify transactions and may face the risk of criminal liability if they fail to comply with the laws . or financial .

D. Legal concepts related to private and anonymous blockchains:

Another important legal challenge is the use of private blockchains or Distributed Private Networks (DPNs) . In this type of blockchain, unlike public blockchains like Bitcoin , access to data and transaction information is restricted to the general public.

This is especially true when privacy - based cryptocurrencies like Monero Or Zcash raises issues related to transparency and accessibility of transaction information.

Private blockchains and private distributed networks are specifically designed to prevent hacking and disclosure of personal information , but at the same time , these features may be easily used by money launderers to hide evidence and financial traces . Therefore , the use of these types of technologies in the fight against money laundering and financial crimes leads to challenges such as data ownership rights , user privacy , and data sovereignty.

3-3.Applied Analysis : Legal and Supervisory Challenges of Money Laundering in Privacy - Based Cryptocurrencies in Different Legal Systems

One of the major complexities in combating money laundering in the area of privacy - based cryptocurrencies is the conflict between the different legal and regulatory approaches in different countries . Each country approaches this problem differently , and these differences can be a serious obstacle to international cooperation and coordinated efforts to combat money laundering.

A. Legal Requirements in the United States and the European Union:

In the United States , the fight against money laundering in cryptocurrencies is overseen by the Financial Crimes Enforcement Network (FinCEN) . This organization specifically oversees the Know Your Customer (KYC) and Anti - Money Laundering (AML) requirements for financial institutions . In this regard , in addition to the fact that digital currency exchanges are required to comply with KYC and AML regulations , more stringent monitoring measures such as Suspicious Activity Reports (SARs) are also required . Or They are also required to have a SAR (Bank Secrecy Act) . Or The BSA , which governs in the United States , is heavily enforced on digital currencies . However , as noted , privacy - based digital currencies like Monero and Zcash are difficult to monitor and track , particularly due to their technological design .

In contrast, in the European Union , new regulations under the Markets in Cryptocurrency Act (MiCA) aim to create A monitoring framework A piece of legislation has been passed for digital currencies . This law requires regulatory authorities to focus on monitoring identity verification and combating money laundering in cryptocurrency exchanges and other financial services . But these laws still face challenges that cryptocurrencies face . They create privacy , they seem inadequate . In particular , no specific method for transparency and traceability of transactions in such currencies is provided in these regulations .

B. Challenges of developing countries and weak regulatory institutions:

In developing countries , these challenges are compounded.Countries like Peru , Pakistan, and Nicaragua , which are under the pressure of economic crises , Countries that are subject to international sanctions may see the use of cryptocurrencies as a way to circumvent financial and international restrictions . In these circumstances , monitoring transactions and tracking money laundering through digital currencies becomes even more difficult . The lack of appropriate legal and supervisory infrastructure , coupled with a lack of specialized human resources , makes it difficult for these countries to effectively enforce anti - money laundering regulations in the area of cryptocurrencies.

In this context , for many of these countries , the main challenge is that regulatory authorities must constantly deal with economic crises , poverty and limited resources , while anti - money laundering laws are usually complex and require precise information analysis . These difficulties make it easy for transparency in digital currency transactions to become a tool for illegal activities.

C. Challenges of Japan and Sou:

In Japan , the FATF and other regulatory bodies are working hard to create laws to prevent money laundering in the world of digital currencies . In Japan in particular , regulators are placing a particular emphasis on transparency , with exchanges and cryptocurrency companies required to register with the government and comply with KYC and AML regulations . In South Korea , strict regulations have also been put in place regarding transaction transparency and user identification . In this country , the use of privacy - based currencies such as Monero and Zcash has been significantly restricted . However , despite strict laws , the use of these currencies in illegal activities has still been reported in these countries.

4. Legal and Regulatory Responses to Money Laundering Challenges Using Privacy - Based Cryptocurrencies

A. Strengthening anti - money laundering (AML) laws and identifying specific risks:

To combat these threats , many countries are strengthening and updating their anti -money laundering laws . For example , in some countries , regulators have required digital currency exchanges to conduct know - your - customer (KYC) and report suspicious transactions . In this

regard , some regulatory bodies , particularly in the European Union and the United States , have enacted laws to mandate transparency in transactions.
B. Using new technologies to identify suspicious activities:
Due to technological advances , some regulatory agencies and blockchain analytics firms , especially in the areas related to digital currency supervision , are using advanced tools for transaction analysis and money laundering detection . These tools can help identify suspicious transaction patterns , even if privacy - based cryptocurrencies are used .
C. Restricting the use of privacy - based cryptocurrencies:
Some countries are looking to restrict or ban the use of privacy - based cryptocurrencies . For example , in Japan and South Korea , these types of currencies are subject to strict laws . These countries are actively seeking to prevent the use of these currencies in illegal activities and are constantly updating their laws.
D. International cooperation to strengthen oversight and law enforcement:
Different countries should strengthen their international cooperation in the field of combating money laundering through foreign currency loans.
Digital continue . Organizations such as FATF and other global oversight bodies can prevent the spread of this type of illegal activity by developing global standards and encouraging countries to adopt and implement anti - money laundering laws in a coordinated manner .

4-1.New techniques for transparency of transactions and combating money laundering

A. Using new technologies such as machine learning and big data analytics:
One of the new responses to the challenges of combating money laundering in the field of digital currencies is the use of machine learning and big data analytics to identify suspicious patterns in transactions . These technologies can automatically identify suspicious patterns in anonymous blockchains and help regulatory authorities track suspicious transactions . Blockchain analytics companies such as Chainalysis and CipherTrace are developing tools that increase the ability to identify and track transactions related to privacy - based cryptocurrencies . These tools use sophisticated methods such as transaction correlation analysis , transaction simulation , and network behavior analysis .
B. Use of chains Focused communication:
Another approach being explored in this area is the use of centralized communication chains that can help regulators track communications between users on privacy - based blockchains . This process is particularly important in decentralized transactions and in the increasingly popular DeFi (decentralized finance) framework .
C. Use of Virtual Private Networks (VPNs) and Private Blockchains:
The use of virtual private networks (VPNs) and private blockchains can also add to the challenges posed by money laundering . Many criminals and money launderers use these technologies to hide

their location and identity . Addressing these challenges requires policies A piece of code for identifying and analyzing transaction data .

5. - Solutions to address money laundering challenges in the field of privacy based cryptocurrencies

Solutions to address money laundering challenges in the field of privacy - based cryptocurrencies
A. Strengthening transparency and identity verification processes in exchanges:
One of the most effective ways to mitigate money laundering risks with privacy - based cryptocurrencies is to strengthen Know Your Customer (KYC) processes and closely monitor transactions on cryptocurrency exchanges . Exchanges should use advanced tools to identify suspicious transactions and enforce strict rules for interacting with customers and suspicious transactions . This not only helps to make transactions transparent , but also prevents privacy - based digital currencies from being turned into tools for money laundering .
B. Supporting research and development in the field of blockchain analytics:
Blockchain analysis One of the most important tools in combating money laundering in the world of digital currencies is . Given the complexity of transactions related to cryptocurrency - based In particular , research and development in the field of creating advanced blockchain analysis tools is essential . Blockchain analysis companies and regulatory bodies should pay attention to They are constantly upgrading their tools to identify hidden patterns in transactions . For example , tools for analyzing precise transactions Zcash Or Monero can be somewhat efficient at identifying and tracking suspicious transactions , although this process still has many challenges .
C. Strengthening international cooperation and information exchange:
Given the global nature of digital currencies , combating money laundering requires extensive international cooperation . To combat money laundering in the field of privacy - based cryptocurrencies , different countries should share data and information on suspicious transactions and suspicious identities . FATF and other international institutions can act as a coordinating authority , encouraging different countries to implement uniform laws and exchange information . In addition , regulatory bodies in different countries should work together to develop coordinated and consistent policies to combat money laundering through digital currencies .
D. Prohibition Or restrictions on the use of privacy - based cryptocurrencies:
Some countries may decide to restrict travel due to security and financial concerns . Or even ban the use of privacy - based cryptocurrencies . In this regard , banning the mining or use of currencies such as Monero and Zcash in certain countries , especially in legal and regulatory areas , may be an effective solution to reduce the use of these currencies in illegal activities . These bans can be among the preventive measures to prevent the spread of money laundering .
E. Establishing international standards for the supervision of cryptocurrencies:
Another effective way to reduce money laundering risks is to develop and strengthen global regulatory standards for digital currencies . Currently , the Financial Action Task Force (FATF) has issued recommendations for the supervision of digital currencies , but these recommendations

are mainly applicable to transparent digital currencies such as Bitcoin and are not sufficient for privacy - based cryptocurrencies . Therefore , new and comprehensive standards for monitoring digital currency transactions should be created and approved by different countries , taking into account their specific characteristics .

5-1.Suggested legal and regulatory solutions

A. Establishing comprehensive and harmonized legal frameworks at the international level:

One of the most important steps to combat money laundering in privacy - based digital currencies is to create A harmonized international legal framework is needed . International bodies such as the FATF and the G20 should seriously work towards regulating and harmonizing anti - money laundering laws in the field of cryptocurrencies . These laws should focus on the effective implementation of systems KYC and AML should be focused on exchanges , wallet providers , and other cryptocurrency financial institutions .

B. Strengthening international cooperation in tracing and tracking suspicious transactions:

In the field of privacy - based cryptocurrencies , international cooperation between different countries to track transactions and information related to money laundering is essential . This cooperation should include international information exchange and the use of advanced analytical tools such as blockchain analysis and machine learning to identify suspicious patterns .

C. Determining the responsibility for the verification of exchange offices and financial service providers:

Effectively combating money laundering in this area requires the establishment of precise legal responsibilities for exchange offices and financial service providers . These responsibilities should be formulated in the form of transparent rules for timely reporting and verification of the identity of their customers , so that even when using privacy - based currencies , suspicious activities can be identified and tracked.

5-1-1. Final Recommendations for Effective Enforcement of Anti - Money Laundering Laws in Privacy - Based Cryptocurrencies

1. Reform and update supervisory laws : Countries should amend their domestic laws , especially in the field of Modify KYC / AML to accommodate the specific characteristics of privacy - based digital currencies and comply with international standards .

2. Use of advanced technologies : Supervisory institutions should use advanced tools to analyze blockchain and identify suspicious patterns in digital currency transactions .

3. Creating international agreements : Countries should cooperate more on information exchange and convergence of anti - money laundering laws in the field of cryptocurrencies .

4. Strengthening the accountability of exchanges : Cryptocurrency exchanges and financial service providers should be held more accountable for transparency of transactions and reporting to regulatory authorities .

5. Maintaining a balance between privacy and financial monitoring : An approach based on preserving privacy rights should be used to effectively monitor transactions and prevent financial crimes.

By following these guidelines and implementing coordinated measures at the international level , money laundering challenges in privacy - based cryptocurrencies can be effectively and legally addressed .

6.Analysis of three legal cases - the crime of money laundering using cryptocurrencies

In the sphere of money laundering using cryptocurrencies, there are a few significant legal cases that we are going to analyze and review. These cases are particularly related to privacy-based digital currencies and the legal challenges arising from the use of these currencies for money laundering. Here are three important cases:

6-1.Monero Money Laundering Case in the United States: The "BitMEX" Case

In 2020, one of the largest anti - money laundering cases involving cryptocurrencies was opened in the United States. The case involved an exchange BitMEX was involved, which operated primarily on the basis of trading Bitcoin and other digital currencies. BitMEX was accused of violating anti - money laundering and know - your - customer (KYC) laws. Of most importance to this case, however, was how digital currencies rely on aspects of privacy, such as Monero, used in suspected transactions for money laundering activity.

In some research into the investigation, the crypto traders of BitMEX were found mainly utilizing digital currency in this regard, named Monero, for masking identities to participate in suspicious transactions. While monero depends on protocols of ring Signatures, RingCT/Ring confidential transactions, in many words it is a technique/technique that holds a transaction cycle secret, name, rank, and identity hidden among the sender, the amount and receivers thereof, making this tracing close to impossible in an appropriate manner by any regulated bodies.

In nutshell, BitMEX was suspected to do money laundering. Precisely, the case emphasized the legal issues in the use of the following cryptocurrency for money laundering that first provided a number of privacy-based transactions: Monero.

6-2. "PlusToken" case and Usage of digital Currencies in money laundering

The PlusToken scheme, one of the most significant to come undone in the world of cryptocurrencies, was launched in China in 2019 and promised people that they would earn enormous sums by investing in cryptocurrencies. The case came to light as a scam and subsequently led to fraud and money laundering charges against its executives.

In this instance, over $3 billion of investors' money was illicitly withdrawn and then laundered. Given that PlusToken used a variety of cryptocurrencies, including Ethereum and Bitcoin, to transact, some of the fraudsters used the privacy-based currencies like Monero in a bid to cover their trails.

This case clearly illustrates how digital currencies, especially those falling under specific sanctions, can be used as tools for money laundering. Chinese regulatory authorities have also imposed strict controls on the use of such currencies in the aftermath of this case.

6-3. The " BTC - e " case and money laundering using digital currencies

BTC-e It was one of the major cryptocurrency exchanges that closed in 2017. This exchange was mainly used for conducting transactions. Bitcoin was well - known and at that time, many illegal transactions were taking place on this platform. It accused the officials of this exchange with money laundering and sponsoring unlawful activities by using Bitcoin and other digital currencies. This investigation showed that one of the methods used in money laundering on this exchange was the use of digital currencies to hide users and financial purposes, especially private ones.

The main defendants in the case were Alexander Vinnik, named as a senior manager of BTC-e, arrested and extradited to the US on charges of laundering over $9 billion through the exchange. Many users used Bitcoin and other cryptocurrencies, such as Monero, to execute transactions in order to veil their identities. Case BTC-e has been a perfect example of how cryptocurrency exchanges turn into major money-laundering platforms, and privacy-based cryptocurrencies come in especially handy in such contexts. This case also shows the prime need for close monitoring and international cooperation in order to trace suspicious transactions across the globe.

BTC-e Exchange Seized and Operator Arrested - US Department of Justice.

Conclusion

Combating Money Laundering in Privacy-Based Cryptocurrencies It is a complex and multifaceted legal challenge that relates to issues such as human rights, national sovereignty, judicial competence, and the responsibility of financial institutions. The specific characteristics of these currencies, especially in the area of privacy and anonymity of users, significantly reduce the ability of supervisory authorities to track and identify suspicious transactions. This issue, especially in the area of anti-money laundering and combating financial crime laws, requires the development of comprehensive and coordinated laws at the national and international levels.

In the meantime, developing or economically stressed countries need a flexible legal framework that will give governments a chance to take advantage of new technologies while at the same time protecting individual rights and privacy. Only by means of international cooperation, under continuous monitoring of such challenges, it will be possible to prevent money laundering from spreading into the world of digital currencies and achieve a transparent and secure financial system.

To address these challenges, a number of key legal actions would have to be considered :

A. Creation of Complete and Harmonized Anti- Money Laundering Laws at the International Level:

One of the most basic requirements in this regard is the formulation and implementation of comprehensive and harmonized anti - money laundering laws at the international level. Given the transnational and decentralized nature of digital currencies, especially those based on proprietary technologies, supervision and control at the national level alone is not enough. Countries should, under the supervision of institutions such as the Financial Action Task Force (FATF), enter into agreements to share financial information and establish legal frameworks. They need to have at least one that will combat money laundering and other financial crimes in space.

To this end, we will be basing our recommendations on : In this regard, the FATF has established mechanisms that ensure cryptocurrency exchanges and platforms are transparent about the transactions, verify the identity of the individuals using their services with AML and KYC laws. For the avoidance of such abuse, the regulations should be revised to accommodate the particularities of privacy-based cryptocurrencies, including Monero and Zcash.

B. Developing advanced surveillance technologies and analytic tools:

One of the main preconditions for enhanced supervision and combating money laundering in the digital currency space is the development of new technologies for analyzing opaque blockchains. These utilities should, therefore, be able to detect suspicious patterns, especially those transaction-based on privacy.

Artificial intelligence, Machine learning, and big data analytics applied in combination with blockchain analytics techniques can, therefore, be powerful utilities for both regulators and law enforcement agencies in identifying and tracking money laundering transactions. These utilities are able to track transactions on private blockchains. Or pseudo - private ones that use private protocols such as zero - knowledge proofs and ring signatures to simulate and identify financial patterns.

C. Increasing accountability for money changers and financial service providers:

From a legal point of view, the exchanges of cryptocurrency and financial service providers shall be legally liable in case of suspicious transactions. Many developed countries under the supervision of the FATF require exchanges to do due diligence processes. The KYC / AML have been put in place to give transparency into who are the users and their finances. However, whether exchanges will be able to trace these transactions remains questionable in light of specific challenges of privacy-based digital currencies.

In this context, it is necessary to develop more precise and comprehensive laws on the responsibilities of exchanges. What is more, exchanges should be obliged, in particular, to file more precise suspicious activity reports with financial and regulatory authorities, and blockchain analysis for suspicious transactions using private and semi-private blockchains. Responsibilities of exchanges should be more precisely identified, especially in cases of transactions that use hidden identities.

D. Development of the legal mechanisms of international cooperation:

The lack of effective international cooperation and information transparency is one of the main barriers to fighting money laundering with the use of digital currencies. Anti-money laundering laws and monitoring of digital currency transactions can be differently organized in different countries. Such discrepancies will encourage a criminal to move to countries with more 'relaxed' laws or to use the services of exchanges, which are located in these countries for the purpose of money laundering.

Mechanisms for international cooperation should be established to help in transparency and the sharing of information about financial transactions. The protocols of cooperation should be concerning the analysis of financial data, combatting financial crime, and the tracking of transactions. The tracking of digital currency and money laundering should be done globally through blockchain analytics platforms. Therefore, it is necessary to promote legal convergence and international cooperation in this field.

E. Protection of privacy rights within the framework of financial regulations:

In terms of the protection of privacy - based cryptocurrencies, respect for privacy, financial transparency, and economic security have to be ensured. In some circumstances, there is a need to devise legal approaches that strike a proper balance between individual rights and regulatory requirements. New legislation should provide powers to the regulatory authorities to act, when the need arises and within the spirit of the principle of minimum intervention, to clarify suspicious transactions, thereby preventing abuse in all its financial manifestations. On the other hand, it should be made certain that these surveillance measures do not cause any harm to the rights of privacy held by a person and violate the very principle of fundamental human rights.

References

1. Albrecht, C., Duffin, K., Hawkins, S., & Rocha, V. (2019). The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control. https://doi.org/10.1108/JMLC-12-2017-0074.
2. Dyntu, V., & Dykyi, O. (2019). CRYPTOCURRENCY IN THE SYSTEM OF MONEY LAUNDERING. Baltic Journal of Economic Studies. https://doi.org/10.30525/2256-0742/2018-4-5-75-81.
3. Finn Brunton.(2019). *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency*. Princeton University Press
4. Lal, B., Agarwal, R., & Shukla, S. (2021). Understanding Money Trails of Suspicious Activities in a cryptocurrency-based Blockchain. ArXiv, abs/2108.11818
5. Maria Conti, Ernesto Damiani,Sushmita Ruj.(2020) "Blockchain Analysis for Anti-Money Laundering: A Systematic Review".*IEEE Transactions on Engineering Management, p42*

   DOI: 10.1109/TEM.2020.2975278
6. Primavera De Filippi ,Aaron Wright.(2018). *Blockchain and the Law: The Rule of Code* Primavera De Filippi, Aaron Wright. Harvard University Press.
7. Robert Johnson , Emily White.(2022). "Global Regulatory Standards for Cryptocurrencies: Challenges and Opportunities" *Journal of International Financial Markets, Institutions & Money/ p66* DOI: 10.1016/j.intfin.2022.101567