THE ROLE OF CRYPTOCURRENCY IN MONEY LAUNDERING: CHALLENGES FOR CRIMINAL LAW

Sakshi Singh*

ABSTRACT

One of the most disruptive forces in digital financial transactions is the rise of cryptocurrency as a "decentralised, safe way of financing transactions and settlement" that provides more pseudonymous business/user solutions. It has a decentralised system that provides fast, cheaper, and more malleable cross-border transactions through blockchain technology. It's the same attributes that make it more desirable for unauthorised users in terms of money laundering. "The decentralised trust element of blockchain technology combined with its anonymity/pseudonymity makes it easy for criminals to fly under the radar so they can get black money turned into white money via complex channels." The paper explains the transactions of cryptocurrencies that offer money laundering services through the various wallets and layering methods. Additionally, the paper explains the utilisation of privacy coins and DeFi as mediums in that vein. Therefore, the paper will delve deeper into the various policing reforms that cryptocurrencies offer regarding jurisdiction and the various challenges that cryptocurrencies pose to the enforcement of criminal law in relation to jurisdiction, fast-paced technological changes and the lack of applicable jurisdiction over cryptocurrencies. The matter at inquiry was centred around proving the inefficacy of the current money laundering acts in relation to emerging threats. The abuse of cryptocurrency can be efficiently addressed through the adoption of a prudent blend of legal, administrative, and tech-based measures. Legal changes would be required to align global legislation and deal with AML legislation in general from the viewpoint of cryptocurrency. Tech-based innovations like superior forms of blockchain analytics capabilities would be essential to curb illicit transactions. Because effective law enforcement and compliance only result from enforcement measures, the paper calls for collaboration with the public and private sectors as well as capacity-building for law

*BBA LLB (HONS.), THIRD YEAR, RASHTRIYA RAKSHA UNIVERSITY, INSTITUTE OF NATIONAL IMPORTANCE, GOI, MHA, GANDHINAGAR.

enforcement agencies. The research brings to light the dual-purpose nature of cryptocurrencies, which contribute significantly to international finance, yet advance criminal abuse. It is suggested that mitigating transboundary impacts through an orchestrated strategic way will enable the use of cryptocurrency while limiting its abuse.

Keywords: Cryptocurrency, Money Laundering, Decentralised Finance, Privacy Coins, Legal Frameworks.

INTRODUCTION

Cryptocurrencies are digital or virtual currencies that use cryptographic techniques for transaction security and control in the generation of new units. The value of cryptocurrencies as opposed to traditional, so-called fiat currencies is that they are decentralised on distributed ledger systems using blockchain technology. Bitcoin, introduced in 2009, will always be regarded and remembered as the foremost in this regard in terms of technological revolution, which followed through numerous others. For instance, Ethereum, Ripple, privacy-focused offerings like Monero and so forth, much to this effect have followed it up unexpectedly within that same year.

Having existed as alternatives for over a decade now, cryptocurrencies have clearly stood out in a most valuable way: they have been a hit with individuals, businesses, and entire governments alike. These have reduced the cost of transferring funds beyond recognition, made the transaction solid as a monument against threats to security, among other factors, and include the periodic changes in the traditional monetary systems. One of the most significant factors that has been outstanding has been the matter pertaining to cross-border money transfers, the impact of the help that cryptocurrencies have brought in banking the unbanked, and, most frightening of all, groundbreaking revelations in the area of DeFi. Nevertheless, with (at least) all of the above came also this intense abuse, in fact. There are many legal uses of cryptocurrencies. However, cryptocurrencies are pseudonymous and lack control. One of the good uses of this cryptocurrency would be to launder money so that it is not traced back to its origins, and such money could then be used as if it had never been misappropriated. It is believed that it would be extremely difficult for police and most other authorities since money launderers could not be caught since they would be transferring money using cryptocurrency.

By utilising several wallets and acquiring cryptocurrencies, the entire trail of transactions is obfuscated, making even further exact evidence gathering difficult for law enforcement, and

using coins such as Monero, Dash, or ZCash that provide an enhanced version of anonymity, defeating law enforcement. Alongside increases in the rise of DEXs, and the development of peer- to-peer platforms, these are likely to make the different regulating and monitoring of illicit activities even more difficult. With the increased usage and trade of cryptocurrencies, the potential for misuse increases, with significant challenges posed to the global financial system and legal frameworks.

ANALYSIS OF CRYPTOCURRENCY'S ROLE IN ML AND THE LEGAL REGIME FIGHTING FINANCIAL CRIME

The purpose of this research will be to find out how cryptocurrencies become a part of money laundering schemes and the problems they create in the enforcement of criminal laws.

Aim: The aim is to study the possible mechanistic and technical methods that might have been used by the criminals and applied for the purpose of money laundering involving cryptocurrencies. To diminish the existing weak capabilities of the anti-money laundering (AML) setups under the anti-cryptocurrency stance of money laundering.

Further, shall the jurisdictional, technical, and regulatory difficulties waylay law enforcement agencies? Such practical solutions will incorporate legal reforms, international cooperation, and higher technological equipment that will mitigate risks associated with ML-based cryptos.

Thereby sieve knowledge on the use of some of these new technologies in the world of crimes and economy, providing judicial enlightenment so that policymakers, regulators, and law enforcement agencies will enhance their contribution in effectively dealing with cryptocurrency use in crime.

How are Cryptocurrencies used in Money Laundering?

Cryptocurrencies have methods that help in money transferring, usually done through precise, sophisticated, innovative ways. Most criminals execute the strategy of layering a transaction with multiple wallets so that the funds' origin may well be hidden. The privacy-focused-cryptos-like, say, Monero or Zcash, have the edge of another layer over their transactions; it becomes almost impossible to trace through their transaction characteristics. Other methods identified come out of contributions from decentralised exchanges (DEXs), which operate in a manner without any central authority, and from blending illegal with legitimate funds through

tumblers or mixers. It will explore these methods, as well as present some practical cases with their implementation.

Which Issues do Cryptocurrencies Create in Existing Criminal Laws?

The underlying issues are about the tradition of law vs. the legal definitions, but in a more specific sense, the very term 'cryptocurrency' has no comprehensive accepted definition within criminal laws. The decentralised, pseudonymous nature of cryptocurrencies presents a challenge to the traditional frameworks of criminal law on jurisdictional issues. Blockchains' nature as global networks often makes the handling--or, really, the hindrance--that any such laws would create in respect to contrary or complementary issues rather difficult for the application of those laws to the global sphere of use. Many of these legal frameworks also provide mechanisms to address this concept of pseudo-anonymity, so there are comprehensive enforcement powers coupled with confusion. In reality, these developments are carried out at unmatched speeds by the evolution of legislation, so there is complete inadequacy on the part of the police regarding the nexus of technology and crime in the crypto-world. It always reveals its weaknesses, which lie somewhere between technology and law enforcement agents.

How might the legal frameworks change to face these challenges?

However, with a view to fighting cybercrime that relies on the use of cryptocurrency, the legal environment necessarily must evolve, resisting the inevitable differences characteristic of a blockchain technology environment. Some of the solutions proposed in such a crisis may involve the international harmonisation of laws relating to AML, which can include compliance requirements for virtual currency exchanges and liability standards of decentralised systems. Advanced integrated analysis capabilities, tools, blockchain analysis, and AI contributions to this integration in creating a legal system capable of enforcing its standards. The collaboration between governments and other organisations represents a major approach to the development of a legal regulatory environment.

Meaning of Cryptocurrency: Encryption-based cryptocurrencies are the introduction of digital assets to the whole value chain called blockchain technology, which allows immutability and transparency. In all transactions, it uses cryptography, which processes any activity and prevents penetration by unwanted actors from middle-interference. Some of the critical features are decentralisation, where a single body is not in charge, and pseudonymity, as the users carry out trade without exposing their real identities.

Popular Cryptocurrencies: Known as the first-seen and the most popular currency, Bitcoin establishes a digital passive medium for transactions. Ethereum was the first blockchain that introduced programmable smart contracts, a logic through which the functionality and business value of blockchain can be leveraged. Privacy-centric cryptos - Monero and Zcash - allow for obfuscated transaction details and are favoured for use in illegal activities.

Trend Analysis and Facts: The current research, as evidenced by the findings, poses an indication of a rising trend in the use of cryptocurrencies for illegal acts. Some recent reports emerging from blockchain analytics firms state that in billions of illicit dollars, the flow passes every year through the use of cryptocurrencies, although this does not categorise the burglarious act to the average percentage of the overall use of the crypto act. The absolute value stands out as a big challenge to the law.

Legal Situations: Current AML Laws: Applicability to Cryptocurrencies: The AML regulations, for example, those specified by FATF, oblige the financial institutions to embrace practices such as Customer Due Diligence (CDD) screening within the widening spectrum of cryptocurrency trading services. This serves to make a revolutionary impact on their classical KYC practices.

Limitations of What Stands as Regulation: These provide for robust efforts; however, they explain some of the gaps that are not addressed by AML laws in the cryptosphere. In cryptocurrency, the concept of the platform being decentralised, peer-to-peer transactioning, as well as the use of privacy coins, is out of the ambit of normal governmental oversight and thus is an arduous thing to implement. In addition, the lack of standardisation in the use of cryptocurrency across the globe provides an opening to exploit its use by wrongdoers. Law enforcement agencies across the globe lack the capacity to monitor the transaction trails on the blockchain.

METHODOLOGY

The research is based on a qualitative study and therefore undertakes an in-depth study based on practical examples and laws. The case of money laundering involving cryptocurrencies is explained in-depth by analysing the case studies. The case study in this research revolves around that particular new scenario, respective working approach, and risks and opportunities in relation to such an offence. Many aspects will be highlighted in relation to this topic, such as harm caused by methodology, financial systems, supporters, terrorism, and laws.

Secondary Sources of Data: The secondary sources of data that will be incorporated in the research include the addition of reputable sources such as government publications, regulatory sources such as FATF and Europol, as well as research sources that offer information on blockchain analysis companies such as Chainalysis. The secondary sources give information on trends, challenges, and best practices in the prevention of money laundering through cryptocurrency.

The case studies are reviewed to demonstrate the different ways money laundering activities occur through cryptocurrencies. These cases can include the well-known Silk Road dark web market or ransomware attacks that demanded payment of a ransom in the form of Bitcoins. By examining these cases, the research is able to point out the flaws in the existing regulation and enforcement.

TRADITIONAL MONEY LAUNDERING AGAINST CRYPTO-BASED COMPARATIVE ANALYSIS

It has a comparative analysis framework that tries to compare traditional money laundering practices that occur through digital systems, such as cryptocurrency money, to those of the conventional money laundering checklist. Such conventional practices, such as that of the well-established principle, have never worked in a way that makes all dirty money clean.

Methods for Money Laundering with Cryptocurrency: Layering with Multiple Wallets and Exchanges: The perpetrators use various accounts that move money in various steps, which increases the difficulty in tracing the illicit money that has been transferred. This process further involved some money exchanges.

Use of Privacy Coins and Decentralised Platforms: These private coins, like Monero and Zcash, take anonymity to another level by concealing information regarding both sender and receiver and regarding the transaction amount. These platforms also work on a decentralised system, which means they do not involve any middleman, and therefore, this whole process becomes more anonymous.

Involvement of Mixing Services, Tumblers, and Darknet Marketplaces: Mixing illegal and legal money makes them untraceable, meaning that none of the money can be tracked because they all lack provenance.

Darknet markets usually support cryptocurrency payments and act as a platform through which the acquisition and sales of illegal products and services take place, acting as another method for money laundering.

Challenges for Detection:

Pseudonymity and the Decentralised Nature: The traditional financial system doesn't need identification disclosure. Cryptocurrencies don't involve names for the users. This is the way the double whammy of pseudonymity and the decentralised nature beats the authorities' capabilities of identifying the illegal parts of the operations they might undertake.

International Flow of Cryptocurrency Transactions: Since cryptocurrency transactions in the blockchain system don't have borders, money laundering by criminals takes on an international dimension as they launder money in different regions to circumvent laws and regulations.

Tracing and Freezing Illegal Money: Cryptocurrencies, being censorship-resistant and nearly freeze-proof, make it relatively difficult for any government to intervene after tracing illegal money. This trail of deception only gets thicker with methods like Privacy Coins and Tumblers.

CRYPTOCURRENCY LAW: OBSTACLES

Jurisdictional Issues: Global nature of crypto transactions: Cryptocurrencies are traded on any one of several decentralised blockchain networks, which operate in a number of global territories. Such transactions between a number of different parties located in different global territories would take several seconds, and they were beyond the walls of finance. In this case, more than one country can be concerned in terms of illicit acts, with various levels of laws to enforce.

Conflicts in International Approaches to Regulation: The disparity within the methodologies applied by nations towards giving responses to the regulation of cryptocurrencies is a criterion for a spectrum, which ranges from the prohibition of specific cryptocurrencies to permission. Since this lack of standardisation creates an arbitrage within regulations, it presents an opportunity for criminal groups with regard to nations with non-existent states of expectation. In addition, since these worlds fail to see eye to eye with regard

to digital currencies, it becomes difficult for them to pool their intellect towards making joint efforts directed at combating money laundering.

Difficulties: Knowledge Deficiency: Good portions of the law enforcement group possess no knowledge in the field of blockchain technology, so that it outpaces anyone with knowledge in this area within them. They would rather have the ability in the areas of blockchain analytics, cryptography, and decentralised systems functioning. Even more unprepared to tackle this case are those who have received inadequate training and resources.

RECOMMENDATIONS

The decline in importance of anti-money laundering regulations through cryptocurrencies, as researched, is the trigger for the realisation of the need for a strategy that encompasses different ways of coping with financial crimes that come from crypto assets. The recommendations for dealing with these problems will follow:

Development of Comprehensive Cryptocurrency-Focused AML Laws: It has been recommended that speciality AML legislation be developed in order to prevent money laundering via cryptocurrencies, and this should be made mandatory for cryptocurrency trading platforms, cryptocurrency wallets, and all other cryptocurrency services as well. All of this should be done as part of the AML and KYC processes.

The heads of the relevant agencies need to ensure that the regulatory environment they have can regulate the centralised and the decentralised platforms, since the latter are used by criminals as a result of the lack of controls. Also, relevant legislation will have to keep pace with these technologies, such as the privacy coins and DeFi projects, so that they do not become hiding places for illegality.

Harmonisation of International Regulations: Considering cryptocurrencies as border-transcending, legislation in information management and money laundering will have to be synchronised on an international level. It would also enhance better co-operation and sharing of information among different countries, especially in light of the fact that the kind of crimes being perpetrated crosses national boundaries and might involve several jurisdictions.

The international bodies involved in the formulation of regulations like those in the Financial Action Task Force (FATF) would have to come to an agreement to set common standards that

may be used by the different countries to see to it that enforcement is not only consistent but also challenging to enforcement efforts.

CAPACITY BUILDING

Defence Staff Training in Blockchain Technology: Full training aid was requested by all the policing agencies of the world, including understanding blockchain technology, including activities that could be undertaken by various cryptocurrencies at the same time, as well as monitoring follies by a press conference on tracing dirty illicit transactions. This is more than knowledge or awareness of the subject, including things such as practical assistance for tracking information, for example, through blockchain analytic tools related to handling transaction information. The development of such courses may also be achieved by constructing a beneficial partnership with software developers in the blockchain with the universities and the relevant professional bodies to suit the agencies.

Cooperation with Blockchain Analytical Firms: This problem was also related to the cooperation between the agency itself and some firms like Chainalysis, Elliptic, and CipherTrace that specialise in CI (Cryptocurrency Intelligence), monitoring cryptocurrency transactions to trace some suspicious actions. They are rated highly on the basis of having sophisticated instruments to further trace the money flowing through multiple blockchains. They can trace and identify signalised indications of effectiveness through intelligence for action. Even faster attention and law enforcement agencies may also need to be called upon in the sector to respond even faster to the emerging challenges.

TECHNOLOGICAL INNOVATIONS

Who Will Manage the Transaction Monitoring Using AI and Machine Learning?

Using AI and machine learning, significant progress has been made in terms of analysing large amounts of data in the blockchain for “anomalous” patterns of transactions, pointing to money laundering to the authorities. They are extremely useful in monitoring large and voluminous transactions, beyond what is physically accomplishable by human staff. The AI technology is most likely to predict risks based on the occurrences of the past and predictive elements of data applied to predict and monitor cryptocurrencies.

CONCLUSION

In recent years, the developments in the Cryptocurrency sector have led to a revolution in the financial sector, and this has been achieved with a tremendous amount of potential and equally poses a significant challenge, especially in the aspect relating to money laundering. It has been shown in this research how money is laundered by criminals through the use of cryptocurrencies in criminal activities, for instance, by layering small amounts, privacy coins, and decentralised platforms. The legal systems and practices have to take into consideration the changes in the financial market in relation to financial crimes.

The perspectives of anti-money laundering that precede all the existing ones within the international community have been used to define the missing link in strategy that exists, which impacts the effectiveness in applying the AML process in fighting cryptocurrencies, as well as any other financial crimes. Such factors like jurisdictional, technological innovations, vacuuming, and a lack of a unified regulatory process have therefore culminated in a rather very friendly environment for the culprits. If more cryptocurrencies continue to thrive, the misuse shall continue to thrive alongside.

In an attempt to curb these problems, the authors are recommending a multi-disciplinary approach that combines some elements of legal reform, some elements of modern technology, and other elements of collaboration between the public and private sectors. In relation to international regulation and the application of technology, there is potential to have an easily regulated atmosphere that fully collaborates with virtual currencies. This would be important in allowing the law enforcement body to be more specific in their approach to the prevention of criminality using efficient technology, such as advanced analytics on the blockchain, combined with current AI technology.

Although the potential for innovation and financial inclusion presented by cryptocurrencies is present, it is fraught with huge dangers that are prone to abuse. The potential present in the world of cryptocurrencies can be utilised to create a much safer and more stable environment for all those who are involved, while being held under control to curb the potential for abuse. The current findings above serve as an eye-opener for all those who are involved to come up with solutions for the new trends in the world of cryptocurrencies and money crimes.