Impact of Digital Currencies and Cryptocurrencies on Money Laundering in India

- Manshi Bhatt

Table of Contents

Abstract

Cryptocurrencies and its increasing prevalence is a topical issue in recent times as it is a decentralised form of currency which completely eliminates the usage of physical cash and thus omits the challenges associated with the conventional physical banking system. While this digitised money has its own advantages, we can not help but talk about the potential financial threats it brings in with it. Cryptocurrencies are a very volatile form of currencies and are not regulated by any organisation making its users vulnerable to various financial frauds. This paper briefly reviews the impact of this new form of tech on the Indian economy and how criminals have targeted it to launder money.

The paper explores the evolution and growth of cryptocurrencies in India and how it has impacted the financial market in the overall world. It delves deeper into how criminals are using this new technology to launder money , incorporating case studies from throughout the world in order to get a better understanding of what steps the Government of India needs to take in order to prevent such scams. By the end of it, the paper focuses on suggesting technological solutions, policies and potential legal frameworks in order to regulate crypto , exercise taxations on the profits generated via it and prevent crimes based on it.

Keywords- *Cryptocurrencies, Money Laundering, Physical banking system, Taxation*

Introduction

The current generation is witnessing an upsurge in the usage of digital currencies worldwide. With the boom in Information and Technology, crypto has become a trending topic. It is estimated that the market size of cryptocurrencies will increase by [1]34.5 billion USD at a CAGR (Compound Annual Growth Rate) of 16.64% between 2023 and 2028.

Talking about India particularly, the fast and cheap internet has made all the data accessible to every citizen at the tips of his fingers. [2]The rise in the usage of mobile payment apps like Paytm and BHIM- UPI has educated people about the possibilities of digital currencies. The Central Bank Legal Currency (CBLC) is a digital currency issued by the Central Bank of India but it is entirely different from other Digital Currencies like Bitcoin, Etherium etc. It has legal tender and thus is equivalent to the value and safety in use just as physical money (The Indian Rupee). On the other hand, cryptocurrencies are also digital currencies only but they are not regulated by any bank or a financial authority. Noticing the latest trends in the market, they are being seen as one of the biggest financial revolutions in recent times. Since cryptocurrencies are not government controlled

---

[1] Expected increase in market size of crypto
[2] Rise in usage of digital currencies

and are relatively a new form of technology, they are accompanied by a high risk of potential financial frauds, money laundering being one of them.

The paper addresses the risk of money laundering via cryptocurrencies/digital money on the Indian market and how India can introduce new effective policies that can help prevent such frauds. At a time when access to the internet is so effortless, it becomes the responsibility of the government to regularly introduce laws to safeguard people from security breaches.

Literature Review

Methodology: For the fulfilment of the objectives as stated in the abstract, this study will rely on the secondary data collected from various sources such as articles, research papers, governmental websites and official legal documents provided by the government of India.

1. A [3]PWC report, "**Future of digital currency in India**", talks about how the world is exploring digital currencies and how the Indian government considers E-Rupee as a revolution in the Indian financial market. The article focuses on the advantages and future of CBDC in India. According to it, this digitised currency can bring structure and stability in the financial system since it automates the process of transactions and acts like a footprint for it making it easier for everyone to carry out day-to-day money exchanges. Though the article provides us with the advantages that come with this kind of system, it fails to shed light on the potential threats that come with it. The frauds are bound to increase if all the transactions take place over the internet. There is still a technological gap present in the nation and the world as a whole which makes this digitised system relatively harder to implement.
2. In 2019, Simon Butler published a research paper " **Criminal Use of Cryptocurrencies- a great new threat or is still cash the king?**", which challenged the Federal Reserve Chairman's statement (July,2018). The chairman said that "Cryptocurrencies are great for money laundering". Butler found that even though bitcoins and other cryptocurrencies can be used for money laundering, cash still is the real issue since the percentage of these crimes carried out via physical money is far greater than that carried out via the digitised money. He made an extreme statement that " Cash is the greatest facilitator of crimes, not cryptocurrencies, and is likely to remain so as long as it exists." Though it is true that physical currency is posing a larger threat today comparatively but completely dissing the probability of cryptocurrencies being the new suitable place for carrying out frauds easily is not right. The technology is still building and we need to be prepared for every type of risk that comes with it.

[3] PWC report

3. The research paper " **How does the Price of Bitcoin Volatility change?**" written by Kurihara and Fukushima in 2018 examines how the volatile prices of bitcoin changes using the empirical method. The results suggest that traders should keep both long term and short term volatility in mind before investing since it is a very risky market to invest in given that its market value fluctuates rapidly (even in minutes).
4. An article on [4]VentureBeat " **Crypto can prevent money laundering better than traditional finance**" states how less than 0.5% of transactions taking place via cryptocurrencies like Bitcoin and Etherium are used for illicit purchases and how blockchain technology can easily facilitate compliance. It focuses on how successful compliance and safe transactions can happen with the existing AML regulatory frameworks. But we can not deny the fact that if cryptocurrencies are not that big of a threat in the present time, it won't be one in the future too. Technology is constantly evolving, in order to minimise the risk it might possess in the future, we should start building technologies to make it even more safe to use.

Overview of digital currencies and cryptocurrencies

In 2009, cryptocurrencies came into existence with Bitcoin becoming the first-ever digital unit with a monetary value that could be used for transactions. [5]In the initial years, its worth was almost nothing but in 2009, Martti miami, a computer science student, sold 5,050 bitcoins for 5.02 USD. This gave each bitcoin a value of 0.0009 USD. As of June 2024, there are more than 25000 other cryptocurrencies in the market. These digital currencies don't have a physical form at all unlike CBLC, they are just the transfer of digital assets. They can be seen as different spreadsheets which carry the information of who owes how much to whom or paid how much to whom. It is a one enormous spreadsheet of every transaction taking place throughout all the computers connected to the network which is also called a Ledger.

Crypto is not regulated by any bank or financial institution, so it's a Decentralised form of currency. For every transaction made in a ledger, there is a copy of that transaction in every computer connected over that network. Due to this, it becomes really easy to track illegal transactions as any sort of phishing gets caught if all the other networks don't show the exact same ledger. This makes it trustable since it is an open traceable transaction system. Another advantage to this kind of currency is that it is secured by cryptography. The biggest example of cryptography that is used by many popular cryptocurrencies is [6]blockchain. Blockchain is a secure way of organising the ledgers of transactions into blocks.

[4] VentureBeat article
[5] Bitcoin price history
[6] Blockchain

Talking about the demerits of this new age currency, it is a very volatile one just like gold. Since its worth is not specified anywhere, its price is prone to intense fluctuations in the crypto market. Another disadvantage of it is that it's not accepted as a payment method in many places and countries. China does not accept cryptocurrency as a real monetary unit and thus has banned its usage in the country. On the other hand many countries like India and New Zealand are still in the processing stage of how they should go about this new technology.

Money laundering: Concepts and Mechanisms

Money Laundering is a process of hiding the origin of money that is illegally earned via frauds, terrorist activities and drug trafficking. In simpler terms, It is a process of making black money white. This illegitimately acquired money is integrated in the economy using various methods and stages. The [7]three stages of money laundering are placement, layering and integration.

1. **Placements**:- It is the first stage of money laundering which is usually done through a series of regular small transactions. It means depositing the large sum of money into the bank by breaking it into smaller sums.
2. **Layering**:- It is carried out by placing the illicit money together with the legitimate earnings. It is usually done by generating so many intricate transactions that the dirty cash disappears into them.
3. **Integration**:- Money laundry carried out via integration of the black money back into the legitimate economy is done by opening businesses like antique shops or non-profit organisations. These businesses are set up to make it look like the money earned is the profit generated by them. The integrated cash is often placed into luxurious assets, properties and long term investments that can be used to accommodate future money laundering attempts too.

The intersection of money laundering and cryptocurrencies

After the onset of a hyper tech era and the introduction of cryptocurrencies, there were speculations of how the loopholes in the digitised monetary system could be manipulated which could result in an increasing number of financial frauds as this technology is relatively new in the market and the knowledge related to it is very limited at the given time. The doubts held true after criminals started laundering money via cryptos.

[8]There are many ways in which money laundering can be done using cryptocurrencies, Smurfing followed by mixing services (tumblers) being one of them. Just like the conventional method of

[7] 3 stages of money laundering
[8] ways of laundering money via crypto

money laundering, smurfing via cryptos also works by making many small transactions of the large sum of money which are distributed across multiple accounts. This account might belong to one individual only but is run by different associates. To obfuscate these transactions, smurfers use various techniques like mixing services and layered transactions. In order to use this money, the smurfers withdraw it in small amounts to make it appear legitimate to the blockchain analytic tools. Doing so makes it harder for the regulators to trace back the original source of these funds.

Other widely prevalent ways to launder money via the digitised currencies are Fiat exchanges, Nested services, Exchange hopping and using blockchains that can hide transactions using advanced cryptographic techniques. In nested services, the criminal makes use of illicit addresses to conduct exchanges. Chain hopping or Exchange hopping involves the conversion of one type of cryptocurrency into another in order to make the traceability of the illicit money complicated. In this, criminals generally break down a huge amount of cryptocurrencies into smaller ones, sending them to multiple addresses to obscure the original source. This process is repeated several times till the laundered money is cashed out on exchanges.

Darknet markets

[9]Darknet markets are the markets operating on the dark web where illegal goods and services are purchased and sold. Even before cryptocurrencies came into existence, these were operating on full scale. But after the introduction of cryptocurrencies in the market, they got heavily dependent on its usage since it ensured anonymity of the user. The criminals generally convert their illicitly earned funds into cryptocurrencies in order to purchase goods on darknet markets due to which the origin of these funds stay anonymous. This makes the process of money laundering smooth and safe for these scammers.

Let's take a look at some real life cases of money laundering that got carried out using cryptocurrencies in the past:-

1. [10]**Bitcoin Fog case**:**-** It was operated by Roman Sterlingov, who used to provide this service to criminals. He was the longest running cryptocurrency "mixer" who helped criminals launder their illicit money from darknet places.
2. [11]**Plus Token Ponzi Scheme:-** This scam resulted in a steep decrease in the prices of bitcoin in 2019. Disguised as a "high return investment program" which offered great rewards to its customers in return to the investments they made, it was a ponzi scheme which made profits by concealing the illicit origins of funds and using them to purchase goods and services in order to make it appear legitimate.

[9] darknet markets
[10] bitcoin fog case
[11] Plus Token Ponzi Scheme

Impact Assessment

While money laundering carried out via cryptocurrencies is relatively lower than the conventional methods of money laundering as it's a new concept , it still imposes a big threat to the economy given that the knowledge related to this field is increasing amongst the people worldwide. Talking about the key trends related to this tech, there is a steep drop seen in the cases of money laundering done via crypto between the years 2022 and 2023. This might be a result of a sudden decrease in the transaction volume between the given time period. Talking about the fiat exchange services, there are thousands of them in operation but most of the money laundering activities are concentrated on a few of them. [12]The black money sent to these off-ramping services increased between the time period of 2022 to 2023 but by only 3%.

Lets see what are the perceptions and attitudes of stakeholders on this matter:-

1. **Financial institutions:-** They have varying opinions on the use of cryptocurrencies and its threats. Some are optimistic about the development of this technology while others are sceptical and concerned about its misuse. If we generalise their opinions as a whole, they think there should be stronger laws for risk management.
2. **Public :-** People are still in the transition phase. Due to the volatile nature of this market and frequent news about the crypto frauds, they are scared of scams and thus don't find it trustworthy. This is because most of the population don't have an understanding of cryptocurrencies.
3. **Government:-** The governments of different countries have different money laundering laws and are still exploring new ways to prevent such frauds. They are also exploring ideas on how to tax these cryptocurrency gains in order to prevent tax evasion.

Regulatory and Legal Framework in India

India's Financial Intelligence Unit (FIU) imposed a fine of 188.2 million rupees ($2.25 million) on the world's largest crypto exchange, Binance, for operating in the country in violation of local anti-money laundering regulations.

[13]India has not enacted any special legislation for the regulation of virtual currencies ("VCs"). However, it has contemporised various statutes like the Companies Act, 2013, necessitating the reporting of virtual digital assets ("VDAs") in an effort to reflect the emerging dynamics of the financial landscape. In 2002, India introduced the **PMLA** (Prevention of money laundering act) which intended to make the hiding of illicitly earned money much more difficult for the offenders. As stated PMLA is "An Act to prevent money-laundering and to provide for confiscation of

[12] chainanalysis
[13] Companies Act 2013

property derived from, or involved in, money-laundering and for matters connected therewith or incidental thereto."

According to it every banking company, financial institutions and intermediaries need to maintain a record of all transactions, whether such transactions consist of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month. Additionally if any governmental authority has a reason to believe that a person has hidden any information about his or her possessions and income then it has the complete right to search that person and seize the illegal possessions if found. That person shall be presented in front of a magistrate within 24 hours of the confiscation.

For decades, the government and the citizens have been concerned about money laundering and after the introduction of cryptocurrencies, the situation got even more tense due to the lack of knowledge in this field. [14] In 2022, India introduced a 30% tax on gains made with crypto currencies followed by the PMLA act amendment in 2023. Now Cryptocurrencies and VDAs also come under the purview of Anti- Money Laundering laws. The transactions involving cryptos and virtual digital assets or VDAs are subjected to regulations in order to prevent frauds related to this tech. The activities such as Fiat Exchanges, exchanging one or more types of virtual digital assets, financial services related to cryptos etc will be supervised. Some of the changes in this system are as followed:-

1. A principal officer should be appointed by the services providers of digital assets.
2. The details of the designated principal officer should be provided to the Financial Intelligence Unit of India (FIU-IND)
3. Suspicious and international transactions, loans and money transfers need to be reported to the Financial Intelligence Unit of India within 7 working days.

The government of India brought this law to widen the taxation and regulatory net and give more power to investigative agencies like ED and ID. However, there are many concerns due to the lack of a central regulator. On March 7, 2023 the finance ministry issued a notification to bring cryptos under PMLA. The aim of this move was to aid investigating agencies to carry out actions against crypto firms. The taxation of VDAs has been included in India's income tax laws, reflecting the fiscal implications of the burgeoning VC market. The government also amended section 271C of the Income Tax Act a month before the amendment of PMLA which made the non-payment of the TDS on VDAs to be a punishable offence. Publicly the cryptocurrency industry largely welcomed the move though they are sceptical that without a central regulator it would not be of any use.

[14] PMLA 2022 Amendment

An updated version of the National Strategy on Blockchain was also released in December 2021, advocating the development of a national blockchain infrastructure.[15]Additionally the government's stance towards VDAs is still awaited, with a proposed bill titled The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021.The government is leading global crypto regulation discussions with the International Monetary Fund and other stakeholders. The Reserve Bank of India (RBI) addressed risks associated with VDAs, including consumer protection, investor safety, market integrity, financial stability, and challenges specific to Emerging Markets and Developing Economies (EMDEs).

Comparative Analysis: International Approaches

[16]The BitMEX Scandal

BitMex was a crypto financial service provider which used to let its customers trade over the digital platforms without disclosing their real identities. It was founded by Arthur Hayes, Benjamin Delo and Samuel Reed. This resulted in an upsurge of illicit activities taking place over the various crypto networks. The founders of this platform were very well aware of the potential issues their services might create but they chose profit over compliance. In 2020, Commodity Futures Trading Commission (CFTC) filed a lawsuit against BitMEX and it faced several criminal charges. The company was accused of defying anti-money laundering laws , operating as an unregistered Futures Commission Merchant (FCM) and failing to abide by the KYC laws.

[17]The Thodex Scandal

Thodex was a turkey based crypto exchange but after 2021 it faced serious criminal charges and was shut down. The abrupt downfall resulted in huge losses of its 4,00,000 customers. The founder of Thodex, Faruk Fatih was found in Albania after a year and was sentenced to 11,196 years in prison. He was charged with fraud, money laundering and many more crimes. This humongous crime created a fearful environment, which made the users of cryptocurrencies reluctant to use this digitised monetary unit. This also resulted in an overall decrease in the usage of cryptocurrencies in the year that followed as we saw in the earlier sections of this paper.

These huge Scandals related to money laundering carried out via cryptocurrencies can be seen as big lessons of how a decentralised digitised currency can also result in extreme financial scams despite being open source. The key takeaways from these incidents are:-

1. The importance of a regulatory organisation and laws are a must.

---

[15] Crypto Bill
[16] The BitMex Scandal
[17] The Thodex Scandal

2. People should be educated enough about cryptocurrencies before they start investing in it since it's a risky deal.
3. India needs robust anti- money laundering laws and KYCs to prevent such mishappenings.

Talking about the aftermath of the scandals, these incidents really eroded the trust of the people investing in cryptocurrencies and made everyone aware of the threats these digital currencies possess. While in the Thodex incident, the government was more focused on punishing the criminals to send a message worldwide, the BitMex incident brought more of a revolution in the market since the government focused on regulatory enforcement actions in the industry as a whole.

[18]United States

In 2022, the US government announced a new framework which sought to empower the SEC (Security and Exchange Commission) and CFTC (Commodity Future Trading Commission). Despite the developments in this legal sector, the US is still finding its way out in order to create balance between protecting the investors and fostering technological developments.

Australia

Australia treats cryptocurrencies legally which means taxes are imposed over the gains associated with it on individual levels. Fiat exchanges can operate freely in the country but they need to be registered with AUSTRAC and comply with AML/CTF regulations. Talking about the future legal reforms in the pipeline, Australia is developing a comprehensive regulatory framework to regulate cryptocurrencies with a potential 12 month transition period after implementation.

Japan

Japan has taken a progressive approach towards this new technology by legalising it under Payment Services Act (PSA). Though all the crypto exchanges must be registered with FSA and must operate in accordance with AML/CFT obligations. In September 2022, the government announced it would introduce remittance rules as early as May 2023 to prevent criminals from using cryptocurrency exchanges to launder money. The Act on Prevention of Transfer of Criminal Proceeds will be revised to allow for the collection of customer information.

India needs to bring in a more defined legal framework for cryptocurrencies since it is a country with such cheap access to the internet. Even the rural areas in this nation have internet connectivity which makes it a leading platform for the prevalence of crypto knowledge and investment. Though India continues to hesitate to ban crypto, it has been working on improving the legal structure as a whole to improve the situation. International cooperation is essential in this, since these digitised

[18] Crypto Regulations around the world

currencies are not bound by any borders. In order to minimise cross- border crypto crimes, an international regulatory body can be a good solution.

Technological Solutions and Innovations

Artificial Intelligence and machine learning are equipped to analyse large sets of data and thus can prove transformational if used properly. The following are some examples on how it can be utilised for the tracking money laundering and other crimes done via cryptocurrencies:-

1. **Blockchain Analysis:-** As we saw earlier in the paper that blockchain is like blocks consisting of ledgers of every transaction taking place over the network of cryptocurrency. Its copy is present in every computer connected over the network making the whole system decentralised and thus safe to an extent. With the use of advanced blockchain analytic tools, every transaction can be traced and thus the identification of any illegal financial activity will become much easier.
2. **Bifurcation of Transactions:-** In 2019, Elliptic published a paper on how AI and Machine learning could be used to classify illicit transactions. They carried out an experiment using Logistic Regression (LR), Random Forest (RF), Multilayer Perceptions(MLP) as classification techniques. The experiment was made scalable using Graph Convolutional Networks(CGN). They created a dataset using Bitcoin's largely available raw transaction data which consisted of about 200k bitcoin transactions over a period of time. They were classified as illicit and licit based on a "heuristics based reasoning process". Accounts which reuse the same address and have a higher number of inputs are commonly associated with legitimate activity. This is because these transactions reduce anonymity for the entity signing the transaction. Similarly, an account that consolidates funds controlled by multiple addresses in one single transaction and in turn reduces anonymity-preserving measures for large volumes of users are likely to be legitimate exchanges.Transactions that were linked to entities such as exchanges, wallet providers, miners, and other reputable sources were classified as licit. Similarly, transactions associated with scams, malware, terrorist organisations, ransomware, Ponzi schemes, etc. were tagged as illicit.
3. [19]**Elliptic2:-** Elliptic published another paper in May,2024 where they used a dataset of 200 million bitcoin transactions which was used to observe if the transactions followed odd patterns and if the cryptocurrencies are converted into cash after the multiple point transactions. They did this to identify whether a specific flow of bitcoins may be linked to money laundering activity. The dataset was designed to help researchers and scientists to build better tools and technologies for combating the money laundering done via

[19] Elliptic and Elliptic2

cryptocurrencies. They used the “Subgraph Representation” technique which is used to analyse local structures within complex networks. Elliptic2 classifies shapes and patterns associated with money laundering and normal financial activity in the subgraphs and labelled them as “illicit” or “licit” accordingly. 3 methods were used to train the model:- GNN,Sub2Vec and GLASS.

These tools and advancements of already existing security technologies can be a vital step towards safeguarding the online citizens of the world from security breaches, financial frauds and illegal fiat exchanges. Apart from AI involvement in this sector, the government also needs to focus on making new policies regarding this issue.

Policy Recommendations

To effectively combat money laundering through cryptocurrency in India, several reforms could be implemented. These reforms would need to address regulatory, technological, and enforcement aspects to ensure a robust and comprehensive approach. Here’s an overview of the key reforms required:

1. **Transparency Policy:-** Make it mandatory for the institutions and individuals involved in the cryptocurrency market to establish TMS (transaction monitoring system) at their computers so that it becomes easier for the government to keep a track of transactions that might look suspicious.
2. **International cooperation:-** Since this tech is not confined to any particular border of a country, digital assets can not be regulated only by a single country if it wishes to do so. An international regulatory body needs to be set up by the cooperation of the governments of various countries from all over the world.
   - Global Coordination: Collaborate with international bodies such as the Financial Action Task Force (FATF) to align with global AML standards and share intelligence on cross-border money laundering activities involving cryptocurrencies.
   - Cross-Border Legal Assistance: Strengthen international legal frameworks to facilitate cross-border cooperation in investigating and prosecuting.The United Nations could play a significant role in this too.
3. **Comprehensive Regulatory Framework and Taxes:-** More defined legal procedures with in depth taxation rules need to be set up for every transaction and fiat exchange taking place via cryptocurrencies. Define and categorise cryptocurrencies clearly within the legal framework, distinguishing between different types of digital assets.
   - Licensing and Registration of Exchanges: Mandate that cryptocurrency exchanges and service providers be licensed and registered with relevant authorities, ensuring compliance with anti-money laundering (AML) laws.

- AML/KYC Compliance: Enforce stringent Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations on cryptocurrency exchanges and wallet providers, similar to those imposed on traditional financial institutions.Digital monetary units are relatively new in the system and have gained popularity recently due to their increasing financial and investment returns over time. This comes at the cost of risks associated with it but this won't stop people from trying it out more. To amplify their safety, laws need to be set up to prevent scammers from looting them.

4. **Different Branch of RBI:-** The Reserve Bank of India is the central bank of the nation which overlooks the monetary policies and financial regulations of the country. But it is conventionally adapted to the physical money circulated in the system . Opening a new branch under it that specifically deals with the digital currencies and its regulations might be fruitful in the long run for India, since the crypto market is expected to rise even more in the upcoming times.
5. **Enhancing Monitoring and Reporting Mechanisms:-**
   - Transaction Reporting Requirements: Require cryptocurrency exchanges to report suspicious transactions to the Financial Intelligence Unit (FIU) or other relevant authorities.
   - Threshold Limits for Reporting: Set lower threshold limits for mandatory reporting of cryptocurrency transactions, ensuring that smaller transactions are also monitored.
   - Real-Time Transaction Monitoring: Implement real-time monitoring tools and systems to track cryptocurrency transactions across exchanges, ensuring timely identification of suspicious activities.

Conclusion

With new technologies coming into existence regularly, it has become a necessity for the Indian government to bring in more preventive measures to protect the right to privacy of its citizens.This research paper demonstrated that even though the cryptocurrencies are decentralised and thus transparent about the financial activities taking place over its network, the potential of abuse is never null. The world is getting more and more connected due to the increased and cheap access to the internet with each passing day. India, just like many other countries, is at a crossroads since it has to balance innovation and financial integrity. The government is taking measures in the right direction but a lot still has to be done. In order to mitigate the risks associated with cryptocurrencies, a robust AML and KYC system needs to be built. Cryptocurrencies have indeed introduced a new era of digitised financial crimes but it's a by-product of technological advancements taking place over the years. Every advancement that takes place comes with many potential threats but that does not mean that the changes should not take place. It's our responsibility to adapt ourselves to the changes taking place around us. There should be a balance between fostering innovation and building institutions to regulate it so that crimes don't take place. Use of artificial intelligence in the right direction can be a great way to protect people from potential scams. Regular adaptation of regulatory frameworks is required to keep up with the rapid technical evolution taking place.

References

1. Global Research and Analytics. June 2017. "Bitcoin: Currency of the future or money laundering vehicle?"
2. Bhavana Sahu and Hariom Divakar. 2023. "Cryptocurrency and its Impact on Indian Economy"
3. Ripudaman Singh TanwarRamjas College,Delhi University. September 2022. "Cryptocurrency and Money Laundering (Indian)"
4. Leopoldo Catania, Stefano Grassi and Francesco Ravazzolo. 2018. "Predicting the Volatility of Cryptocurrency Time–Series"
5. Vandana Ajay Kumar. 2012. "Money Laundering: Concept, Significance and its Impact"
6. PRAVEEN KUMAR (University of Delhi). 7 July, 2015. "Money Laundering in India: Concepts, Effects and Legislation"
7. Prevention of Money Laundering Act, 2022
8. Yutaka Kurihara1 and Akio Fukushima. 2017. "The Market Efficiency of Bitcoin: A Weekly Anomaly Perspective"
9. Saifedean Ammous. 2017. "Can cryptocurrencies fulfil the functions of money?". The Quarterly Review of Economics and Finance.
10. Preetham Kumar Boominathan and Guna Sekar Srinivasan. August 2023. "The Impact of Cryptocurrencies on Anti-Money Laundering and Counter- Terrorist Financing"
11. Elliptic (2020). The Future of Crypto Crime: The 2020 Crypto Compliance Report.
12. KuCoin annual report 2022
13. Simon Butler. 2019." Criminal Use of Cryptocurrencies- a great new threat or is still cash the king?"
14. Kurihara and Fukushima. 2018. " How does the Price of Bitcoin Volatility change?"