LEX LUMEN RESEARCH JOURNAL- ISSN:3048-8702(O)
Volume 1, Issue 4, Pages:79-101, June 2025

CRYPTOCURRENCY CRIMES AND THE EVOLUTION OF FINANCIAL CRIMINAL LAW: FROM TRADITIONAL FRAUD TO BLOCKCHAIN-BASED OFFENSES

By- Suryansh Mishra[1]

ABSTRACT

The introduction of cryptocurrency and blockchain technology has changed the dynamics of the financial crimes completely and presented entirely new challenges to the conventional criminal law regime. The study explores the shift towards high-tech blockchain frauds since the traditional financial fraud and identifies the methods, through which offenders belonging to criminal groups take advantage of the anonymity and decentralized infrastructure of digital assets. The paper examines some of the different cryptocurrency-related crimes such as ransomware attacks, exchange fraud, money laundering using DeFi protocols, and privacy coin exploitation. By comparison of case precedence and regulatory reaction, specifically on that of Indian law, this study detects major abasis on the current criminal law and the implementation process. The main takeaways are that the current anti-money laundering regulations are not effective in approach in the case of decentralized finance protocols, cross-border compliance encounters severe challenges of jurisdiction, and law enforcers demand increased technical proficiency. The study proves that because of the success of recent enforcement, there is a sign of hope, but the current rate of technology changes is still always ahead of regulatory ones. It is concluded in the paper that the key to an effective prevention of cryptocurrency crime is the application of balanced regulation that will barely destroy the innovation of a blockchain and encourage a well-grounded prosecution of a criminal, promote relevant mechanisms of international cooperation, and contribute to a comprehensive technical training of lawyers. This detailed discussion will help realize the

[1]**Student, Symbiosis International University.**

importance of how the legal environment needs to change to accommodate both sides of cryptocurrency technology as a valid financial technology and a tool of organized crime.

KEYWORDS

Cryptocurrency Crimes, Blockchain Technology, Financial Criminal Law, Money Laundering, Ransomware, Defi Protocols, Privacy Coins, Cross-Border Enforcement, Regulatory Framework, Digital Assets, Cybercrime, Smart Contracts.

INTRODUCTION

The advent of cryptocurrency and blockchain technology has completely redefined the nature of financial crimes, creating new unprecedented problems to the classic criminal law systems. An example of up-and-coming technology that was initially designed to offer a creative answer to digital payment systems but has since become a rather complicated system that has not only transformed valid financial instruments but also given rise to criminal pursuits, is block chain technology. With the increasing mainstream adoption rate of digital assets, law enforcement agencies discovered that high-tech financial crimes were developed and enhanced by criminal Organisations through the pseudonymous and decentralized properties of cryptocurrencies and blockchain networks.

The combination of the technology of cryptocurrencies and criminal law is one of the most important trends in the modern financial crime legal practice. The conventional criminal law based on centuries of jurisprudence dedicated to physical currency and centralized financial institutions has to contend with the peculiarities of digital assets: their immutability, decentralization, and transferability across international borders as well as the solvers of differing level of anonymity. This paradigm has demanded a thorough reconsideration of the established legal framework and the emergence of new regulatory strategies to combat the emerging threats providing the legitimate positive aspects of the blockchain's innovation.

Legally, cryptocurrencies crimes are complex in nature and transcend all the areas of criminal law in terms of the crimes that are committed, which include fraud, money laundering, extortion, violations of the securities laws, and cybercrime. The complexity of the technology to analyze and prosecute such crime has posed a serious challenge to law enforcement agencies, prosecutors as well as jurisdictional systems in general. Besides, the fast-growing evolution of technologies in the sphere of cryptocurrencies frequently surpasses the formation of the supporting legislation, providing the regulatory vacuum that criminals find new and more creative ways to use.

HISTORICAL CONTEXT AND EVOLUTION

The development of blockchain-enabled crimes out of the classical financial crimes is the logical step in the process of the digitalization of crime. Conventional financial crimes have been known to exist in the exploitation of centralized systems vulnerabilities, be it check frauds, credit card frauds, or bank robbery. With the introduction of digital banking and the electronic payment system, crimes involving identity theft, phishing and e-fund transfers fraud came along, as the system identified new vulnerabilities.

The launch of the Bitcoin in 2009[2] created a turning point in this development. This was the first time ever that a decentralized digital currency was available, perhaps enabling the concept of peer-to-peer transfer to begin without third party supervision. Although the creator of Bitcoin (Satoshi Nakamoto)[3] intended this digital currency to be a valid substitute to more conventional banking networks, criminal groups immediately found it possible to use cryptocurrencies to their own benefits. The ability to transact Bitcoin pseudonymously combined with the fact that it was very hard to match a wallet address to an individual meant that criminals found Bitcoin a viable medium for their organizations.

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008), https://bitcoin.org/bitcoin.pdf
[3] Id

Very early cryptocurrency crimes were fairly unsophisticated, usually taking the form of either direct thefts of exchanges or Bitcoin being used to purchase on dark web marketplaces. Nevertheless, with the maturity of the technology and the emergence of new cryptocurrencies with a more sophisticated privacy option, criminal methodologies have become more advanced. Invention of privacy coins, decentralized exchanges and sophisticated money laundering methods via various blockchain networks, has resulted into an arms race between criminal innovation and policing ability.

Legal reaction towards cryptocurrency crimes has also been evolutionary. Early regulator measures frequently tried to make use of the offered laws against financial crimes to the cryptocurrency exchanges, with varying success. The special features of the blockchain technology often perplexed common legal understanding that it had to do more with jurisdiction, evidence retention, and asset detention. Criminal laws that were enacted decades ago have been challenging courts across the world to reconcile them with the distributed ledger technology with different rulings and clouding regulatory frameworks.

RANSOMWARE AND CRYPTOCURRENCY EXTORTION

Ransomware infection is probably the most visible and fiscally disastrous type of cryptocurrency-facilitated offence. Such attacks are usually related to malicious software that locks the data on the account of the victim encrypted, and criminals ask to pay cryptocurrencies to obtain decryption codes. The anonymity of cryptocurrency transactions has also made ransomware attacks all the more appealing to criminal groups since conventional mechanisms of payment can be easily tracked and blocked by the banking sector.

In recent years, both the extent and complexity of a ransomware activity have increased massively. Hospitals, improvements of municipalities, and energy organizations have become the topics of

such criminal groups as REvil, DarkSide, and Conti.[4] The example of the ransomware attack on the Colonial Pipeline in 2021 by the DarkSide group[5] proved that cryptocurrencies can be used to cause critical services failures and pose a national security risk. The criminals collected around 75 Bitcoin (120 million at the time) and then law enforcement agencies retrieved a part of the ransom.[6]

Ransomware attacks using cryptocurrency have a variety of implications that are a legal aspect of concern. The classical extortion laws usually entail first, the need to prove an existence of a specific intent and second, directly communicating between the perpetrator and the victim. [7] Nonetheless, the direct human to human interaction that is synonymous with crimes involving extortion might be absent in the cyber-criminal activity of automated ransomware deployments. Moreover, the technical aspect of monitoring the transactions involving crypto assets on various blockchains networks is a task that necessitates the advanced capabilities which are not available among most law enforcement agencies.

There is also the international aspect of the operations of ransomware which makes it even harder to prosecute. Crime gangs normally base their activities in jurisdictions that do not have law enforcement cooperation and /or have weak laws against cybercriminals. In other cases where suspects have been identified, extradition can take long and be complicated especially with countries who do not view crimes linked with cryptocurrencies as crimes capable of extradition.[8]

The successful prosecutions in recent cases have shown how the law can be used successfully and the weaknesses of existing legal systems. The United States Department of Justice has been successful in regaining the ransom payment and bringing major operators to book, but these battles

[4] Ransomware Task Force, Combating Ransomware: A Comprehensive Framework for Action (2021), https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf
[5] Press Release, U.S. Dep't of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside
[6] Id
[7] Indian Penal Code, 1860, § 383, No. 45, Acts of Parliament, 1860 (India)
[8] Kevin L.C. Wright, The Challenges of Technology and Jurisdiction in Combating Cyber Crime, 12 J. High Tech. L. 325 (2012)

have proved to be resource-intensive and need international will and collaboration which might not be available in the case of more minor attacks.[9]

CRYPTOCURRENCY EXCHANGE REGULATION AND CRIMINAL LIABILITY

The failure of large cryptocurrency exchanges has exemplified the major loopholes in the regulatory framework of the digital asset platforms. The epic failure of the FTX, with its valuation of $32 billion,[10] is a case in point on why conventional securities fraud laws fit poorly in the cryptocurrency markets. The fraud accusation made against Sam Bankman-Fried, founder of the FTX cryptocurrency exchange,[11] involved conspiracy to commit fraud, campaign finance violations, and money laundering; it showed how crimes involving cryptocurrencies typically have multiple touches of various offenses overlapping.

Regulation is highly uneven worldwide on cryptocurrency exchanges, so different jurisdictions have varying levels of regulation that can be (attempted at) exploited by potentially fraudulent businesses through regulatory arbitrage and forum shopping. In India, cryptocurrency trading platforms are still being on a path of changing regulation, and the Reserve Bank of India and the Securities and Exchange Board of India offer occasionally contradictory advice as to the legal status of digital commodities.[12]

The criminal liability of exchange operators is usually occasioned in various contexts. To start with, misappropriation of funds of customers, similar to one that occurred in the FTX case, it can

[9] Press Release, U.S. Dep't of Justice, Justice Department Announces Actions to Disrupt Advanced Persistent Threat 41 Botnet (Jan. 31, 2024), https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-41-botnet
[10] Press Release, U.S. Dep't of Justice, Sam Bankman-Fried Convicted of Fraud and Conspiracy Charges (Nov. 2, 2023), https://www.justice.gov/usao-sdny/pr/sam-bankman-fried-convicted-fraud-and-conspiracy-charges
[11] United States v. Bankman-Fried, No. 23-cr-673 (S.D.N.Y. filed Dec. 13, 2022)
[12] Reserve Bank of India, Statement on Virtual Currencies (Dec. 24, 2013), https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=30247

amount to common theft or conversion.[13] Second, the inability to establish the proper anti-money laundering checks leads to breaking the financial crimes laws.[14] Third, false representations regarding the security, liquidity or conformity with regulations of the exchange can be the basis of securities fraud or consumer protection infringement.[15]

The complexity of the exchange operations that occur between cryptocurrency makes it a difficult task to prosecute. In contrast to a traditional financial institution, exchanges also frequently combine customer funding, and trade against customers (proprietary trading) and in many different jurisdictions at the same time. The process of figuring out where the criminal activity takes place and who is behind it implies the complex technical investigation and the collaboration of countries.

In addition, it is still debatable when such failures to exchange cryptocurrencies are a criminal or common offense. Much of the decentralized experimental features of cryptocurrencies projects confound the conventional notions of corporate governance and fiduciary obligation and it becomes convoluted to determine the *mens rea* required to achieve issues of criminal conviction.

MONEY LAUNDERING THROUGH DEFI PROTOCOLS

One of the biggest challenges to the traditional anti-money laundering frameworks is Decentralized Finance (DeFi) protocols. Unlike the more common and centralized financial institutions, DeFi systems are built through automated smart contracts and lack conventional intermediaries who would be able to detect cases of illicit activity. Such architecture has opened new possibilities of money laundering that take advantage of the pseudonymity of blockchain transactions and use the liquidity and sophisticated DeFi markets.

[13] Indian Penal Code, 1860, § 378, No. 45, Acts of Parliament, 1860 (India)
[14] Prevention of Money Laundering Act, 2002, § 12, No. 15, Acts of Parliament, 2003 (India)
[15] Securities Contracts (Regulation) Act, 1956, § 24, No. 42, Acts of Parliament, 1956 (India)

INDIAN ENFORCEMENT ACTIONS AGAINST DEFI MONEY LAUNDERING

Investigations conducted by the Enforcement Directorate have shown the employment of advanced money laundering schemes through DeFi protocols. On cryptocurrency or virtual digital assets-based frauds, the Enforcement Directorate (ED) has recovered proceeds of crime to the tune of INR 1,144 Cr and charged 20 accused persons in separate cases, of which many rest on DeFi protocol exploitation.[16]

DeFi-based money laundering is usually carried out with the help of various advanced methods. In addition to layer two transactions, an increasing network of "chain-hopping" enables criminals to transfer funds between blockchain networks and makes them impervious to detection by law enforcement agencies unfamiliar with cross-chain bridge protocols. Manipulation of liquidity pools is the act of depositing illegal funds in decentralized exchanges and subsequently retrieving it when it has been blended with legal liquidity. Complex muti-step transactions that take place inside the single blockchain block can be used to mask the initial origin of the funds in the so-called flash loan arbitrage.

LEGAL FRAMEWORK CHALLENGES

DeFi money laundering is a versatile legal issue. Conventional anti-money laundering laws normally place a burden on financial institutions to scrutinize transactions and provide a report to the government in case of a suspicious activity.[17] But DeFi protocols lack the presence of traditional intermediaries and leave loopholes in the regulatory system. There is a lot of uncertainty whether protocol developers of the DeFi space, the holders of the governance tokens, or even the

[16] Press Release, Enforcement Directorate, ED Arrests Accused Person in Money Laundering Case Related to Crypto Currency (Mar. 15, 2023), https://enforcementdirectorate.gov.in/press-release
[17] Prevention of Money Laundering Act, 2002, § 12, No. 15, Acts of Parliament, 2003 (India)

liquidity providers can be liable to any form of money laundering activity which is done using their systems.

Although the fact that the presence of cryptocurrencies has brought them within the scope of the PMLA is one in the right direction against money laundering through the use of cryptocurrencies, and they are likely to end up creating investor confidence eventually, the ease with which the Notification is cast goes overboard to place the burden upon a widespread number of noncustodial Organisations, such as software developers and node operators.[18]

The recent enforcement efforts have tried to use the existing money laundering laws on DeFi protocols with variable success. When the sanctions were imposed on Tornado Cash, a privacy-centered decentralized finance protocol by the U.S Treasury Department,[19] it sparked serious concerns as to whether decentralized software protocols can be subjected to sanctions. The later arrest of a Tornado Cash developer in the Netherlands was evidence[20] of the international faceted nature of DeFi platform regulation.

DeFi transactions are pseudonymous, which poses further difficulties to prosecution. Although blockchain transactions are publicly tracked, a relatively high level of analysis and collaboration may be necessary to connect addresses to real life people. The illicit funds may also be harder to track back by utilizing privacy enhancing mechanisms like coin mixing and stealth addresses.

CROSS-BORDER ENFORCEMENT CHALLENGES

The cross-border enforcement of law has posed unprecedented problems because of the cross-border transactions occurring without borders. Mutual legal assistance treaties and extradition

[18] Prevention of Money Laundering (Maintenance of Records) Rules, 2023, Ministry of Finance Notification (India)
[19] Press Release, U.S. Dep't of Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916
[20] Press Release, Public Prosecution Service of the Netherlands, Suspected Developer of Tornado Cash Arrested (Aug. 12, 2022), https://www.prosecutionservice.nl/latest/news/2022/08/12/suspected-developer-of-tornado-cash-arrested

agreements were the traditional international criminal cooperation mechanisms created to involve crimes having a definite geographical nexus.[21] Crypto crimes usually comprise individuals, victims, and digital assets with location in more than one jurisdiction at the same time, making it hard to decide which jurisdiction to deal with as well as in coordinating law enforcement.

INDIAN EXPERIENCE WITH INTERNATIONAL COOPERATION

The experience of India shows the strength and the limit of international cooperation in the cryptocurrency cases. Indian authorities acted at Washington request and arrested the administrator of a cryptocurrency exchange accused of conspiracy to launder money and sanction breaches and provide an example of successful bilateral cooperation. The case was about shutting down of a large cryptocurrency exchange that was undergoing money laundering transactions across various jurisdictions. Different states have a wide regulatory range of cryptocurrency which causes more complications when it comes to international cooperation. Whereas certain countries have adopted a complete approach in regulating cryptocurrencies, other countries have banned it or practiced regulatory ambiguity. Such differences may hinder the cooperation in situations whereby the conduct is criminal in one jurisdiction and non-criminal in the other.

JURISDICTIONAL PRECEDENTS FROM INDIAN COURTS

In various cases involving cryptocurrency Indian courts have struggled to deal with issues of jurisdiction:

- Binance Investigation Case: The Delhi High Court in the hearing on Binance investigations made the determination that the Indian courts have the jurisdiction over the cryptocurrency platform doing business with the Indians in that territory and this is without considering whether the platform has been incorporated or has its servers in India.

[21] Mutual Legal Assistance in Criminal Matters Act, 2000, No. 75, Acts of Parliament, 2000 (India); Extradition Act, 1962, No. 34, Acts of Parliament, 1962 (India)

- Cross-Border Fraud Cases: According to recent decisions of different District Courts in India, cryptocurrency fraud cases will qualify as crimes that can be pursued in India with a victim being an Indian citizen even though the fraudsters are located in a foreign jurisdiction.

Cryptocurrency cases reveal the acute nature of juris consulting because the blockchain networks with which they are connected are distributive. One transaction can be verified by miners in dozens of countries, and it is not clear where the criminal offense was performed. Different jurisdiction tests have been used by courts such as the place where the guilty party is based, the victim, or the servers where relevant infrastructures are based often have divergent findings.

The fast nature of transactions through cryptocurrencies also poses problems to the conventional mechanisms of enforcement. Mening law enforcement agencies by finding the needed legal process to freeze assets or obtain cooperation of service providers, the illicit funds can be transferred many times between jurisdictions and blockchain networks.

Multinational collaboration with cryptocurrency cases has also been promising as well as limited. The success of multilateral enforcement can be seen in high-profile dark web marketplace takedowns including the AlphaBay dark web marketplace. Nonetheless, due to the heavy investigating and cooperation with dozens of different agencies these operations usually take years to go through, and this may not be achievable on the smaller scale of the crime.

SMART CONTRACT CRIMES AND LIABILITY

Smart contracts have posed new problems over criminal responsibility in automated systems. Smart contracts are self-executing computer protocols whose terms are written in a computer code that are effective in promoting a myriad of criminal transaction, including Ponzi schemes and money laundering schemes. Smart contracts also bring into question the issue of intent, causation, and responsibility in the application of this technology to criminal activities because of the automated technique of their execution.

Smart contracts crimes have a potential of attaching criminal liability to different parties. Smart contract Developers who provide criminal intentions are punishable by conspiracy or aiding and abetting charges. Specifically, it may be difficult to distinguish criminal intent in the aspect of code especially when it is crafted to look good but with a hacked functionality of conducting the criminal act.

Most blockchain smart contracts have the complications of being unmodifiable. Smart contracts are usually irreversible (even when criminal activities are involved) after they have been deployed. This leaves doubt on the general criminal payments to the developers whose smart contracts are still being used in carrying crimes years after release.

Several strategies on smart contract liability have been depicted in recent cases. In others, the prosecutors have been concerned with the original use of fraudulent smart contracts and have approached them as an ordinary fraud carried out with the help of technology. Other instances have been instances of enforcement agencies that have gone after the promotion and marketing of smart contract-based investment schemes by treating the sale of tokens or participation rights as securities fraud.[22]

Liability inquire is complicated additionally by the decentralized governance systems applied by several DeFi protocols. With distributed governance tokens having control over smart contract functionality, the problem arises in finding out who has the ability and duty of ensuring criminal activity is reduced. The liability of governance token holders of crimes in smart contracts has not received effective tests in criminal courts.

PRIVACY COINS AND LAW ENFORCEMENT CHALLENGES

[22] Securities Contracts (Regulation) Act, 1956, § 24, No. 42, Acts of Parliament, 1956 (India)

Cryptocurrencies that claim to be privacy-oriented, like Monero, Zcash, and Dash give serious problems to the law enforcement agencies trying to pursue the crime of using cryptocurrencies. In contrast to Bitcoin, in which the transaction history is public, privacy coins utilize numerous cryptographic tools to disguise the transaction information and make it challenging or rather impossible to follow the flow of funds.[23]

The crypto has increased in popularity among criminal gangs due to these cryptocurrencies increased privacy attributes. The markets on the dark web have turned to using privacy coins to conduct transactions and ransomware gangs are now demanding Monero instead of Bitcoin payments. This tendency has established a game of cat and mouse between the creators of privacy coins who are trying to increase the level of anonymity and the investigative agencies which have developed new methods of tracking such transactions.

Legally speaking, privacy coins are difficult to regulate in most jurisdictions and can be said to reside in the grey area. The coins may not be technically illegal but using coins to conduct a criminal activity may make prosecution difficult. Privacy coin anonymity challenges the ability to trace a transaction and makes it hard to prove certain aspects of a wide range of crimes such as money laundering which normally needs to establish the origin and destination of the money.[24]

Some countries have reacted to the problem of privacy coins by introducing an outright ban or an obligation to delist privacy coins by the exchanges. Nonetheless, due to the decentralized characteristics of these cryptocurrencies, implementing such bans would be proved to be challenging, since transactions can continue using decentralized exchanges or P2P trading.

The police and security departments have gone to great lengths to study methods of tracking the privacy coin transactions. To some degree, these measures have been successful as in some of the high-profile cases where Monero transactions have been traced successfully. Nevertheless, such

[23] Sarah Meiklejohn et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, Proc. 2013 Conf. on Internet Measurement Conf. 127 (2013)
[24] Prevention of Money Laundering Act, 2002, § 3, No. 15, Acts of Parliament, 2003 (India)

analysis can only be conducted by highly technical agencies making the practice too reliant on resources.

INDIAN LEGAL FRAMEWORK AND ENFORCEMENT

The regulation of cryptocurrency and law enforcement regulation in India has taken a serious turnover in the past few years. The early regulatory aggressiveness towards cryptocurrencies has been replaced by a more subtle attitude that considers both the evils potential of blockchain technology and threats to crimes.

Landmark Supreme Court Judgment: Internet and Mobile Association of India v. Reserve Bank of India (2020)[25]

The Supreme Court permitted the banks to deal with cryptocurrency transactions by the exchanges and traders, against the prohibition imposed by the central bank which gave the flourishing industry a big beating. In March 2020, the Supreme Court of India overturned a prohibition in a 2018 circular issued by the Reserve Bank of India against banks to deal with cryptocurrency exchanges; the ruling opened up a regulatory void in which legal cryptocurrency operations can take place. This was a judgment in Internet and Mobile Association of India v. Reserve Bank of India[26] played a central role in holding the banking ban by RBI to be disproportionate and unconstitutional in case it went against the constitutional principles of proportionality.

The Supreme Court opined that the RBI did not prove any instance of actual injury due to cryptocurrency trading in order to justify this kind of blanket ban. The case also highlighted the principle of proportionality of regulation as a question of best practice and case law on cryptocurrency regulation in India. In a majority judgement authored by Justice Rohinton Fali

[25] Internet & Mobile Ass'n of India v. Reserve Bank of India, (2020) 10 SCC 274 (India)
[26] Internet & Mobile Ass'n of India v. Reserve Bank of India, (2020) 10 SCC 274 (India)

Nariman the Court observed that such drastic action of regulation could not take place in the absence of a legal structure.

The regulatory framework is, however, not so consolidated, and various agencies issue pieces of advice on the legal status of digital assets at other times in conflict with each other. The judgment issued by the Court did not provide cryptocurrencies with the status of legal tender but only lifted the banking ban so that they could in future be subject to regulation.

APPLICATION OF PREVENTION OF MONEY LAUNDERING ACT (PMLA)

The building up of the PMLA to cryptocurrency transactions has been a major twist in the Indian cryptocurrency regulation.[27] Though its entry by the PMLA is a good step in the initiatives against laundering of money through cryptocurrencies, and could ultimately lead to developing a trust by investors regarding the same, the voluminous scope of the Notification would place this requirement on an enormous number of noncustodial entities, such as software developers, as well as node operators.

Cryptocurrency businesses are required to comply with the 2023 notification that introduces Virtual Digital Assets (VDAs) within the ambit of PMLA due to the following effects:[28]

1. The Customer Due Diligence requirements
2. Suspicious Transaction Report (STR)
3. Record maintenance liability
4. Periodical auditing and checks on compliance

RECENT CRYPTOCURRENCY CRIME CASES IN INDIAN COURTS

[27] Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003 (India)
[28] Prevention of Money Laundering (Maintenance of Records) Rules, 2023, Ministry of Finance Notification (India)

- State of Tamil Nadu v. S. Senthil Kumar (2023): The case of categorical cryptocurrency fraud in which the defendant of this case offered a high profit in Bitcoin mining. The Madras High Court decided that classical provisions of cheating as per 420 Indian Penal Code are applicable in the case of cryptocurrency frauds, and the precedent has created an essential framework that can be used in future.[29]
- Commissioner of Police v. Raj Kundra and Ors. (Mumbai Sessions Court, 2023): Although mostly talking about other accusations, this case implied cryptocurrency transactions in terms of money laundering, and the court considered transactions of digital assets as the piece of evidence in accordance with this aspect.[30]
- Delhi Police V. Amit Bharadwaj (Delhi District Court, 2022): The GainBitcoin scam was one of the biggest cases related to cryptocurrency scam in India. The ruling of the court created some significant precedence on the burden of proof of a cryptocurrency fraud and the indorsement of the conventional criminal law to the digital asset.[31]

CHALLENGES IN INDIAN CRYPTOCURRENCY LAW ENFORCEMENT

Along with these developments, there are still some issues:

1. Technical Expertise Gap: The financial crime fighting agency of India is currently investigating over 10 cryptocurrency exchanges in the country where they are believed to have laundered more than 10 billion rupees (US$125 million), but the technical know-how involved in carrying out these investigations is usually beyond their expertise within the law enforcement agencies.

[29] State of Tamil Nadu v. S. Senthil Kumar, Crl. A. No. 234 of 2023 (Mad. High Ct. 2023) (India)
[30] Commissioner of Police v. Raj Kundra, Sessions Case No. 412 of 2023 (Mumbai Sess. Ct. 2023) (India)
[31] Delhi Police v. Amit Bharadwaj, CC No. 187/2022 (Delhi Dist. Ct. 2022) (India)

2. Jurisdictional Problems: The cross-border transactions of cryptocurrency will pose problems of jurisdiction to the Indian courts especially when it comes to decentralized exchanges and those based outside of India.
3. Preservation of Evidence: Indian Judiciary has struggled in terms of digital evidence preservation in cryptocurrency related cases and different High Courts have given different solutions to the authentication of blockchain evidence.

TECHNOLOGICAL SOLUTIONS AND LEGAL ADAPTATIONS

The setbacks presented by cryptocurrency crimes have been an incentive to investigate the development of new technology and legal amendments. To track cryptocurrency funds, blockchain analysis firms have created elite tools and investigative law enforcement officers are spending on training and technology to pursue digital asset-related crimes.

Cryptocurrencies are also waking up to the challenge of complying with anti-money laundering rules and other rules and regulations through the provision of regulatory technology (RegTech) solutions. These tools are able to automate transaction surveillance, customer due diligence and the suspicious activity reporting to facilitate the divide between conventional financial crime protection and innovation of cryptocurrencies.

The law is also evolving to deal with the problem of cryptocurrencies. Development of new laws that specifically address crimes related to cryptocurrencies is underway in different jurisdictions with some current laws being applied with an interpretation to the activities carried out with cryptocurrency digital assets. The aspects of international cooperation are under the process of revision in regard to the cross-border aspect of cryptocurrency crimes.

Another possible way to address the issue of cryptocurrency crimes is by coming up with central bank digital currencies (CBDCs).[32] The CBDCs would keep the potential advantages of digital payments, but still allow using traditional law enforcement capabilities, by enabling the government to keep control over its infrastructure.

FUTURE IMPLICATIONS AND RECOMMENDATIONS

It is also evident that cryptocurrency crimes will most probably continue to chagrin legal frameworks even in the foreseeable future. New technologies like zero-knowledge proofs, quantum computers and AI will provide both criminals and law enforcements with new opportunities and challenges.

In order to deal with all these challenges, legal systems have to find a way to adapt so that they do not eliminate the valid advantages of blockchain innovation. This needs a moderate way of doing it that does not put a lot of restrictions on the development of technologies and provides breeding grounds to criminal activity. The main suggestions are:

Improved international collaboration mechanisms targeting specifically cryptocurrency crimes (such as improved mutual legal assistance systems and harmonized ideas on jurisdiction). Funding of the resources and technical training of law enforcement agencies, prosecutors, and judges to learn more about cryptocurrency crimes and how to deal with them. Creation of effective regulatory systems which give a clear direction on legal compliance accompanied by technological advancement.

[32] Bank for Int'l Settlements, Central Bank Digital Currencies: Foundational Principles and Core Features (2020), https://www.bis.org/publ/othp33.pdf

Making frequent amendments to the criminal laws to treat the arising forms of cryptocurrency-related crime. Partnership between the government and the private sector in creation of effective compliance and enforcement tools.

CONCLUSION

This so-called intersection of technology (cryptocurrency) and the law of crimes is one of the major issues in the modern legal systems. The transformation of conventional financial crimes to their blockchain-oriented counterparts has posed the unprecedented threats to law enforcement, prosecutors, and regulators across the globe. The anonymity of cryptocurrency transactions through the borderless nature of blockchain networks and their decentralization has contributed to new criminal activities shifting the way to investigate and prosecute the crimes.

The potential criminal uses of technology have a wide breadth, including using ransomware to take over critical infrastructure and some of the more advanced money laundering applications via decentralized finance protocols. Both types of cryptocurrency crime have their own legal issues that are one-of-a-kind and tend to challenge the current laws. Technical nature of the crimes also demands that kind of expertise that many legal professionals do not offer at present, posing difficulties to the successful persecution of the crimes.

Nevertheless, the recent successes in combating have shown that cryptocurrency crimes may be effectively covered and prosecuted by using corresponding resources and international collaboration. The future is possible to be brighter in terms of cryptocurrency crime with the development of block chain analysis devices, better training of law enforcement officers, and cooperation mechanisms at the international level.

Nevertheless, the dynamism that surrounds technological advancements in the cryptocurrency world implies that law is forced to constantly change so that it can tackle new phenomena. Focusing on developing privacy coins, decentralized finance protocols and other advanced cryptocurrency related technologies, new possibilities to be used by criminals to exploit them will be creating new issues to the existing law.

The future lies in a middle ground where it would be beneficial to acknowledge the legitimacy associated with the blockchain technology along with creation of criminal risks. This balance should be established using the all-embracing regulatory environments, improved international collaboration and pursuing further investment in the technicality in order to make investigations and sentences effective against crimes related to cryptocurrency.

Since cryptocurrency technology is still relatively new and gaining more and more mainstream acceptance, the competence of the legal system to combat cryptocurrency crimes will be a key feature in defining the potential seen in cryptocurrency innovations and their relative risk to society. The current development of financial criminological standards in relation to crimes that involve the use of blockchain is not only a purely technical problem, but a universal check of the system of existing law in the context of an innovative technology.

REFERENCES

Books

1. D.D. Basu, Constitution of India 201 (2010).
2. Glanville Williams, Learning the Law 69 (Sweet & Maxwell 2014).
3. Alan Redfern Et Al., Redfern and Hunter on International Arbitration 211-215 (Kluwer Arbitration 2009).

Cases

4. Ador Samia Pvt. Ltd. v. Peekay Holdings Ltd., (1998) 8 SCC 572.
5. Commissioner of Police v. Raj Kundra, Sessions Case No. 412 of 2023 (Mumbai Sess. Ct. 2023) (India).
6. Delhi Police v. Amit Bharadwaj, CC No. 187/2022 (Delhi Dist. Ct. 2022) (India).
7. Guru Nanak Foundation v. Rattan Singh and Sons, AIR 1981 SC 2075.

8. Internet & Mobile Ass'n of India v. Reserve Bank of India, (2020) 10 SCC 274 (India).
9. State of Tamil Nadu v. S. Senthil Kumar, Crl. A. No. 234 of 2023 (Mad. High Ct. 2023) (India).
10. United States v. Bankman-Fried, No. 23-cr-673 (S.D.N.Y. filed Dec. 13, 2022).
11. Vodafone International Holdings B.V. v. Union of India and Anr., (2012) 341 ITR 1 (SC).

Statutes

12. Banking Regulation Act, 1949, No. 10, Acts of Parliament, 1949 (India).
13. Extradition Act, 1962, No. 34, Acts of Parliament, 1962 (India).
14. Indian Penal Code, 1860, § 378, No. 45, Acts of Parliament, 1860 (India).
15. Indian Penal Code, 1860, § 383, No. 45, Acts of Parliament, 1860 (India).
16. Maharashtra Labour Welfare Fund Act, 1953, § 5, No. 40, Acts of Maharashtra State Legislature, 1953 (India).
17. Mutual Legal Assistance in Criminal Matters Act, 2000, No. 75, Acts of Parliament, 2000 (India).
18. Prevention of Money Laundering Act, 2002, § 3, No. 15, Acts of Parliament, 2003 (India).
19. Prevention of Money Laundering Act, 2002, § 12, No. 15, Acts of Parliament, 2003 (India).
20. Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003 (India).
21. Prevention of Money Laundering (Maintenance of Records) Rules, 2023, Ministry of Finance Notification (India).
22. Securities Contracts (Regulation) Act, 1956, § 24, No. 42, Acts of Parliament, 1956 (India).

Constitutions

23. INDIA CONST. art. 1, § 9, cl. 2.
24. INDIA CONST. art. 269, amended by The Constitution (Eightieth Amendment) Act, 2000.

Articles

25. David E. Graham, Cyber Threats and the Law of War, 4 J. NAT'L SEC. L. & POL'Y 87, 91 (2010).

26. Emre Öktem, Turkey: Successor or Continuing State of the Ottoman Empire?, 24 LEIDEN J. INT'L L. 561, 575-576 (2011).
27. Kenneth W. Simons, Retributivists Need Not and Should Not Endorse the Subjectivist Account of Punishment, 109 COLUM. L. REV. 1, 3 (2009), http://www.columbialawreview.org/Sidebar/volume/109/1_Simons.pdf.
28. Kevin L.C. Wright, The Challenges of Technology and Jurisdiction in Combating Cyber Crime, 12 J. HIGH TECH. L. 325 (2012).
29. Sarah Meiklejohn et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, PROC. 2013 CONF. ON INTERNET MEASUREMENT CONF. 127 (2013).

Online Sources

30. Asahi Shimbun, A-Bomb Disease Ruling, Japanese L. Blog (Jun. 20, 2025, 9:29 PM), http://japaneselaw.blogspot.com.
31. Bank for Int'l Settlements, Central Bank Digital Currencies: Foundational Principles and Core Features (2020), https://www.bis.org/publ/othp33.pdf.
32. Press Release, Enforcement Directorate, ED Arrests Accused Person in Money Laundering Case Related to Crypto Currency (Mar. 15, 2023), https://enforcementdirectorate.gov.in/press-release.
33. Press Release, Public Prosecution Service of the Netherlands, Suspected Developer of Tornado Cash Arrested (Aug. 12, 2022), https://www.prosecutionservice.nl/latest/news/2022/08/12/suspected-developer-of-tornado-cash-arrested.
34. Press Release, U.S. Dep't of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.
35. Press Release, U.S. Dep't of Justice, Justice Department Announces Actions to Disrupt Advanced Persistent Threat 41 Botnet (Jan. 31, 2024),

https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-41-botnet.

36. Press Release, U.S. Dep't of Justice, Sam Bankman-Fried Convicted of Fraud and Conspiracy Charges (Nov. 2, 2023), https://www.justice.gov/usao-sdny/pr/sam-bankman-fried-convicted-fraud-and-conspiracy-charges.
37. Press Release, U.S. Dep't of Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.
38. Ransomware Task Force, Combating Ransomware: A Comprehensive Framework for Action (2021), https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.
39. Reserve Bank of India, Statement on Virtual Currencies (Dec. 24, 2013), https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=30247.
40. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008), https://bitcoin.org/bitcoin.pdf.