



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.



WHITE BLACK
LEGAL

EDITORIAL **TEAM**

Raju Narayana Swamy (IAS) Indian Administrative Service **officer**



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru

and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



Senior Editor

Dr. Neha Mishra



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

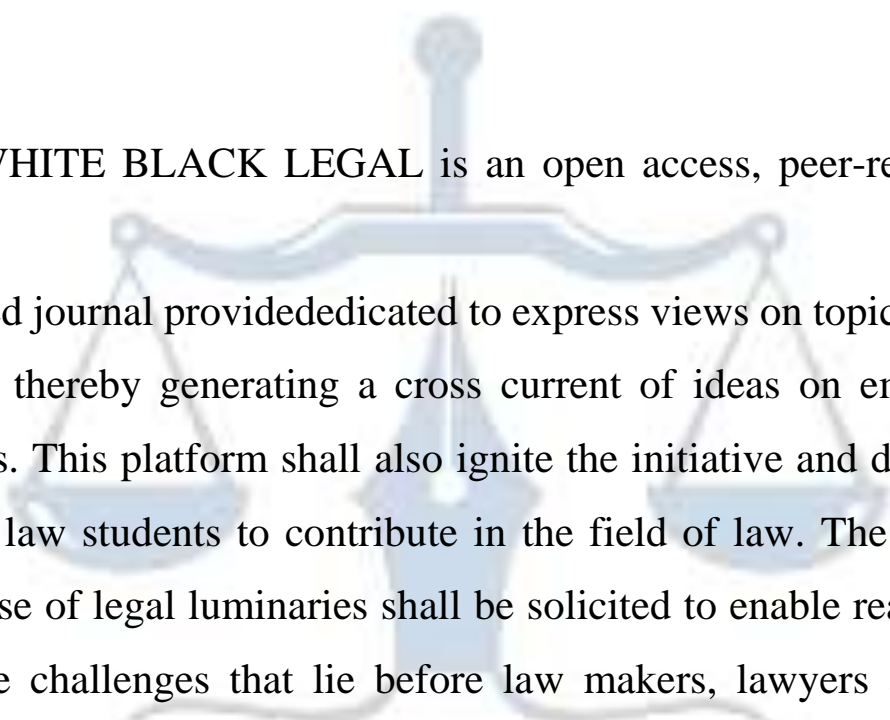


Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US



WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

ROLE OF CRYPTOCURRENCY IN CYBER CRIME

AUTHORED BY - VAISHNAVI M & MATHIARASAN M

Sastra Deemed to be University

ABSTRACT:

This research paper aims to show that the cryptocurrencies are used as an instrument of committing the crime, especially cybercrime. The rapid adoption of cryptocurrency has revolutionized the financial landscape, providing new opportunities for legitimate transactions while simultaneously facilitating a rise in cybercrime. This paper explores the dual edged nature of cryptocurrencies, highlighting their role in enabling various illicit activities such as Crypto jacking, money laundering, ransomware attacks and fraud. Dealing with physical currency is useless for cybercriminals since they might be located anywhere in the world, distant from their victims so they preferred crypto currency as a platform or tool to commit cybercrime. Cybercriminals are drawn to cryptocurrencies like Bitcoin and Ethereum because they function on decentralized networks and are not governed by a single entity. Furthermore, we review the efforts made by the government and regulatory bodies worldwide to curb the misuse of cryptocurrency in cybercrime such as AML regulations, Know your customer policies and blockchain analytical tools. Current data, noteworthy incidents, and patterns in the illegal use of cryptocurrencies are all reviewed in this paper. Ultimately, this research aims to provide a comprehensive understanding of the intersection between cryptocurrency and cybercrime and challenges faced by law enforcement and regulatory bodies in combating cryptocurrency related crimes. Since it is much simpler for the cybercriminals to hide their operations and the source of their assets, we may conclude that the organized criminal underworld is very interested in cryptocurrencies and their appeal among regular, honest persons.

KEYWORDS – Cryptocurrency, cybercrime, bitcoin and Monero, crypto jacking, money laundering, ransomware and digital currency.

INTRODUCTION:

Cryptocurrency and its intersection with cybercrime are a story of technological advancement, innovation, and evolving criminal activity. Cryptocurrency began in the late 2000s, driven by the ambition to create a decentralized, peer-to-peer digital cash system.¹ The concept of digital currency existed prior, but it wasn't until the introduction of bitcoin in 2009 by the pseudonymous creator Satoshi Nakamoto that cryptocurrency became a reality.² In recent years, cryptocurrencies have emerged as a transformative force in the global financial landscape. With features such as decentralized control, privacy and transparency, digital currencies have created new opportunities for legitimate financial innovation. However, these same features have also presented unique challenges for cybersecurity and law enforcement. The anonymity and ease of transactions provided by cryptocurrencies have attracted the attention of cybercriminals, who use digital assets to facilitate illicit activities including money laundering, ransomware, crypto jacking and other illicit activities.³

As cybercrime increasingly incorporates cryptocurrency, law enforcement agencies and financial regulators face hurdles in preventing cybercrimes. This paper aims to explore the role of cryptocurrencies in cybercrime, analysing how they are utilized by cybercriminals and the complexities they introduce to crime prevention. By examining the current landscape of cryptocurrency related cybercrime, as well as existing and proposed guidelines, this research seeks to contribute to a broader understanding of the relationship between crypto currencies and cybercrime.

LITERATURE REVIEW:

Julija Lapuh Bele highlighted that cryptocurrencies are attractive to both risk-averse investors and the criminal underworld and also discussed regarding the third party mining, cyber blackmail, types of cryptocurrencies used to commit the cybercrime and the aspect of trading with cryptocurrencies.

Feng et al (2021) suggests that money laundering using cryptocurrency has grown significantly, with sophisticated schemes utilizing cross chain transactions, mixing services, and

¹ TrendSpider (2023) The history of cryptocurrencies

² Kaspersky. (2024). What is Cryptocurrency and How Does it Work?

³ Bele, Julija Bele, J. (2021) 'Cryptocurrencies as facilitators of cybercrime', SHS Web of Conferences, 111, Article 01005

privacy coins to evade detection.

Greeshma.K.V. mentions that innovation in the pace of development of new currencies and technologies continue to create ongoing challenges for responsible users of technology and regulators alike. This paper also explored that crypto currencies have been linked to various types of crimes such as attacks on businesses, child exploitation, corporate espionage, fake ids and passports, sexual exploitation etc.

Zohar (2020) stated that while some countries have taken proactive steps to regulate or even ban cryptocurrencies, others have struggled to keep pace with the evolving nature of cryptocurrency technology.

Christin (2013) and Foley et al (2019) have highlighted how cryptocurrencies serve as a convenient vehicle for criminal organisations to convert illicit funds into more opaque forms of financial assets.

Barratt et al. (2019) explored the role of digital currencies in drug trade transactions, where cryptocurrencies provided an layer of anonymity for both vendors and buyers.

RESEARCH PROBLEM:

The lack of legal recognition and regulation for cryptocurrency in India results in an inability to regulate and combat cybercrimes involving digital currencies, posing significant challenges for law enforcement and justice mechanisms.

RESEARCH OBJECTIVES:

- To examine the types of cybercrimes where cryptocurrency is commonly used.
- To analyse how the cybercriminals use such cryptocurrencies to commit crime.
- To explore the challenges faced by Indian regulatory bodies in tracking and regulating cryptocurrency transactions linked to cybercrime.
- To propose policy recommendations for India to address the misuse of cryptocurrency in cybercrime.

RESEARCH QUESTION:

1. How does the absence of legal recognition for digital currencies in India impact the regulation and prosecution of cybercrimes involving cryptocurrency?
2. What are the challenges faced by Indian law enforcement agencies in addressing cybercrimes involving digital currency due to regulatory gaps?
3. What potential measures could India implement to regulate cryptocurrency and reduce its use in cybercrimes without undermining innovation in the digital currency sector?

RESEARCH METHODOLOGY:

This paper is a doctrinal research methodology and is based on the secondary data collection and analysis from various research papers, websites, newspapers, article journals, government publications and case studies.

CRYPTOCURRENCY AND ITS DEVELOPMENT:

A Cryptocurrency is a digital or virtual money that may be used to purchase goods and services. There is no physical coin or bill but every transaction takes place through online. It uses cryptography to protect transactions and a decentralized mechanism to record transactions and issue new units rather than a central issuing or regulatory body. The first cryptocurrency was Bitcoin which was introduced in 2009 and it is still in existence. The other cryptocurrencies are Ethereum which was developed in 2015 is a blockchain platform and it was introduced after the Bitcoin. Litecoin is similar to bitcoin, it develops new innovation and processes to allow more transaction. Cryptocurrency have certain benefits like it does not involve third party like bank or government, it is always easy to use and easily accessible by anyone, the payments can be made quick and fast compared to other payment settlements. The receiver and sender hold their private keys and the transactions are protected between these two people with encryption.⁴

Data-driven versions of money storage, digital wallets are where the cryptocurrency users store their money. The blockchain, a publicly accessible peer-to-peer ledger, is actually where all cryptocurrency transactions are kept. Cryptocurrency gets its name from the intricate security process known as cryptography, which keeps the currency safe. It totally depend on the computer network to work and does not rely on third party like banks or government to control

⁴ Rauch, S. (2024) 'The growing relationship between cryptocurrency and cybercrime'

or administer it.⁵ Cryptocurrency is a serious threat to physical currency and banks have a problem in imposing cryptocurrency systems as they are decentralized and are not subject to government control.

CRYPTOCURRENCY IN INDIA:

The Indian government opinion towards cryptocurrency is different from rest of the world. India has neither regulated the cryptocurrency nor banned the use of it. Cryptocurrency was first introduced in India with the paper publication named “Bitcoin- A peer-to-peer Electronic cash system” published by Satoshi Nakamoto in the year 2008. Then the use of cryptocurrency was started in the year 2010 in India when someone utilized 10,000 bitcoins to buy two pizzas. Meantime, the bitcoin earned the value of money and other cryptocurrencies such as Litecoin, Namecoin and Swiftcoin was also introduced in the 2011.⁶ Soon the cryptocurrencies started to gain their position in India and exchange platforms such as Pocket bits, Coinsecure, Koinex and Unocoin and Zebpay started to develop and the Reserve Bank of India issued a warning circular regarding the risk pertaining in the cryptocurrency in the year 2013.

The experiment of demonetization gave a boost to crypto investments and the banks in India started to allow crypto exchanges which in turn forced the Reserve bank of India to release another circular in 2017 stating that virtual or digital currencies are not a legal tender. The Central Board of Digital tax recommended a draft prohibition on Cryptocurrency use to the finance ministry in 2018, and the Reserve bank of India ultimately banned it. Soon after this incident crypto exchanges and virtual currencies fall by 99%. The ban of cryptocurrency is a huge breakdown which made the crypto exchanges file a writ petition in the Supreme Court and it was resulted in declaring the RBI circular as unconstitutional. Still the issue for cryptocurrencies is not yet over.

INTRICATE RELATIONSHIP BETWEEN CRYPTOCURRENCY AND CYBERCRIME:

Cryptocurrency is a digital currency which is easily transactional compared to physical currency. It need not be carried around where ever we go instead all the transaction can be undergone through online. This method of ease access attracted 2 classes of masses. They are

⁵ Investopedia, 2024. Cryptocurrency Explained With Pros and Cons for Investment

⁶ Cavendish Professionals, 2024. The evolution of cryptocurrency

– Terrorists and criminals.⁷ This currency often playing both a role in facilitating criminal activities and serving as a target for crime. They choose this type of virtual currency to commit various types of crimes. So, there is an intricate relationship between cryptocurrency and cybercrime. The role of cryptocurrency in cybercrime raises day by day. The cybercriminals use virtual currency as a tool or instrument to commit crime as because of the high degree of anonymity factor and the user's identity and the transaction between the receiver and the sender remains confidential. This confidential transaction help them to transfer the currency from one country to another in a fast and quick manner. The main reason why the cybercriminals and terrorists prefer cryptocurrency is because of absence of third-party interactions as crypto currencies are not yet recognised by the central bank or government.⁸

TYPES OF CRIMES INVOLVING CRYPTOCURRENCY:

CRYPTOJACKING: Crypto jacking is a type of cyberattack where hackers hijack a victim's computer, smartphone or other devices to mine cryptocurrency without their knowledge or consent.⁹ In a crypto jacking attack, the attacker secretly installs malicious software on the victim's device or tricks them into visiting a website or clicking on a link that runs mining scripts in the background. Attackers can deliver crypto jacking scripts through infected software, phishing emails or by embedding them on websites. The attacker's digital wallet receives the Cryptocurrency that was mined. Because cryptocurrency transactions are typically anonymous, it can be difficult to trace or stop the attack.

RANSOMWARE ATTACK: A ransomware attack occurs when a cybercriminal takes over a victim's computer and encrypts their files, rendering them unreadable.¹⁰ In order to obtain the decryption key that would enable the victim to access their data once more, the cybercriminal will next demand a ransom in the form of cryptocurrency, typically bitcoin.

DARK WEB AND ILLICIT MARKETS: Cryptocurrencies like bitcoin have long been the primary form of currency in dark web markets where illicit goods and services such as drugs, weapons and stolen data are bought and sold.

⁷ Anusha, M.J. (2022) 'Study on cryptocurrency and cyber law: a legal perspective', International Journal for Legal Research and Analysis, 2(5)

⁸ SOCRadar Cyber Intelligence Inc. (2024) The Intricate Relationship Between Cybercrime and Cryptocurrency

⁹ INTERPOL (2024) Cryptojacking

¹⁰ Foley, S., Karlsen, J.R. & Putniņš, T.J. (2019) 'Crypto currencies and cybercrime', Journal of Financial Crime, 26(4), pp. 1029-1042

ROMANCE SCAMS: Romance scams are a type of cybercrime where criminals create fake profiles on social media sites, dating apps or email, posing as romantic interests to gain a person's trust. Once they have established a relationship, they manipulate the victim into sending them cryptocurrency or making risky investments.¹¹

PONZI SCHEMES: Cryptocurrencies have been used fraudulent schemes where victims are lured by promises of high returns, only to lose their investments.

MONEY LAUNDERING: Criminals often use cryptocurrency mixing services, anonymous wallets or decentralized exchanges to obscure the money's origins, allowing them to eventually convert it into legitimate currency without detection.¹² This process exploits the decentralized and pseudonymous nature of cryptocurrency, making it a common tool for cybercriminals.

IS CRYPTOCURRENCY LEGAL IN INDIA?

Cryptocurrencies like Bitcoin, Ethereum etc., is legal in India but it is not yet recognized as a legal tender. Cryptocurrencies are regulated by the Reserve Bank of India (RBI), The Securities Exchange Board of India (SEBI), and the Ministry of Finance.¹³ There is a lack of regulatory framework for trading and holding cryptocurrencies. The Indian government is working on a framework to control cryptocurrency in the country and handle related issues and hazards. Although, people can own and trade digital assets, they cannot be used for regular domestic transactions because they are not accepted as legal cash. The Indian government introduced "The Cryptocurrency and Regulation of Official Digital Currency Bill" in 2021.¹⁴ The measure aims to outlaw all private cryptocurrencies and offer a structure for the Reserve Bank of India (RBI) to issue a CBDC. The bill's provisions are still being discussed and debated, though, and it has not yet been signed into law. The absence of legal recognition of cryptocurrency became more advantage for cyber criminals to commit crime.

Various crimes such as money laundering, ransomware attacks, romance scams, Crypto jacking are committed by the cybercriminals using virtual currency or cryptocurrency. Though, the cryptocurrency is not a legal tender - The criminals and the terrorists committing fraud and

¹¹ Holt, T.J. & Bossler, A.M. (2016) 'The online romance scam: A serious cybercrime', *Crime, Law and Social Change*, 66(3), pp. 313-333

¹² Tookitaki, 2024. *Cyber Crimes and Their Connection to Money Laundering*

¹³ KYC Hub, 2024. *Cryptocurrency Regulations in India*

¹⁴ Tambe, N. (2024) 'Crypto Bill India: What Is Crypto Bill & How It Works', *Forbes Advisor India*.

scams using this crypto cannot be punished by the legal authorities. So, the absence of legal recognition of cryptocurrency in India significantly affects the regulation and prosecution of cybercrimes involving cryptocurrency.

CHALLENGES IN REGULATING CRYPTOCURRENCY AND PREVENTING CYBERCRIME:

The efficiency of cryptocurrency regulation is hampered by a number of challenges, notwithstanding regulatory attempts. Because cryptocurrency transactions are pseudonymous, it is difficult for law authorities to track down and identify anyone engaged in illegal activity. Furthermore, the international character of Bitcoin transactions complicates jurisdiction because different nations have different laws, which can result in regulatory arbitrage and disputes over territorial sovereignty. Furthermore, governmental reactions are frequently outpaced by the quick speed of technology improvements in the Bitcoin industry.

Cybercriminals benefit from this regulatory delay since they can take advantages of legal loopholes and weaknesses without being discovered. India faces a shortage of cybersecurity resources and infrastructure, which impacts its ability to prevent and cybercrime effectively. The main challenge is that there is lack of consumer awareness. Many citizens are unaware of the risks associated with cryptocurrency investments and other related scams, making them vulnerable to cybercrime. Indian Enforcement agencies always face the difficulty in recovering the cryptocurrency asset as they can be quickly moved across wallets or converted into other digital currencies. They also face challenge in tracing and freezing crypto assets which becomes the burden for Indian enforcement agencies. Some cryptocurrency exchanges operate outside India or refuse to cooperate with authorities due to privacy concerns or fear of regulatory backlash. Without cooperation from exchanges for transaction tracking or Know Your Customer data sharing, agencies struggle to connect illegal transactions to specific individuals.

POSSIBLE MEASURES TO REGULATE CRYPTOCURRENCY AND TO PREVENT CYBERCRIMES ARE:

India has taken a number of actions described in a recent report by the Financial Action Task Force (FATF) in an effort to strengthen its defenses against cybercrime and improve the

regulation of virtual assets.¹⁵ Indian Government have established various cybercrime reporting portals and cybercrime coordination centre to prevent cybercrimes. Though there is a requirement for proper legal framework to regulate cryptocurrency and to prevent cybercrimes.¹⁶ Cybercrimes can be prevented by avoiding clicking on various clickbait, spam links, free offers or unsolicited ads which may lead to hacking of your digital wallet. Firms can use software to detect suspicious transactions that may indicate money laundering. Governments may develop Central bank Digital currencies (CBDCs) as a regulated digital alternative to cryptocurrencies, providing the benefits of digital currency while allowing greater control and oversight over financial transactions. Cryptocurrency like Monero prioritizes privacy and makes transaction tracking more difficult so regulators may think about limiting the use of privacy coins or mandating more monitoring in some areas. Use strong passwords, installing anti-virus software, avoiding use of public wi-fi and keeping the system updated are some of the possible measures to prevent cybercrime using cryptocurrency.

LEGAL ISSUES IN REGULATING CRYPTOCURRENCY AND PREVENTING CYBERCRIME:

The regulation of cryptocurrency and the prevention of cybercrime raises several complex legal issues. They are:

Lack of Clear Regulatory Frameworks:

Many jurisdictions are yet to establish clear and comprehensive regulations for cryptocurrencies, leading to uncertainty around how to classify and tax these assets. Cryptocurrencies may be considered commodities, currencies, or securities, each of which involves different regulations. The decentralized nature of blockchain technology complicates jurisdictional issues, as the regulatory authority is not always clear for assets that can be created, held, and transferred globally.¹⁷

Anti-Money Laundering (AML) and Know Your Customer (KYC) Requirements

Cryptocurrency transactions can be pseudonymous, making it difficult for authorities to track the movement of funds. Criminals can exploit this to launder money or finance illegal activities.

¹⁵ Anand, V. (2024) 'India strengthens cybersecurity, crypto regulations to combat rising threats: FATF Report', CNBC TV18, 19 September

¹⁶ Press Information Bureau, 2022. Prevention of Cyber Crimes. Ministry of Electronics & IT. 27 July

¹⁷ International Journal of Reviews and Research in Social Sciences (2019) 'Cryptocurrencies and consumer protection', International Journal of Reviews and Research in Social Sciences, 7(2), pp. 1-13

Regulators globally are increasingly demanding that crypto exchanges implement strict AML and KYC measures, yet decentralized exchanges and certain wallet services remain challenging to regulate, as users can retain a high level of privacy.

Investor Protection and Market Manipulation

Cryptocurrency markets can be volatile and vulnerable to manipulation (e.g., pump-and-dump schemes), making it easy for bad actors to deceive retail investors. Legal frameworks aimed at consumer protection, such as those requiring disclosures and safeguards, are often lacking in crypto markets, making it difficult to prosecute those who engage in fraud or market manipulation.¹⁸

Privacy Concerns and Surveillance

In trying to regulate crypto for transparency, regulators often advocate for increased surveillance of transactions. However, this raises privacy concerns, as such measures could infringe on individuals' rights to privacy in their financial dealings. Privacy-focused cryptocurrencies (like Monero and Zcash) challenge regulators further, as they are designed to prevent tracking of transactions, making it harder to enforce regulations.

Intellectual Property Rights and Digital Asset Ownership

With blockchain assets like NFTs and other tokenized forms of value, issues arise around intellectual property (IP) rights, copyright, and asset ownership. NFTs can raise questions about the legal ownership of digital media, as copyright laws may not always extend to tokens, creating ambiguity for owners and creators.

Jurisdictional Challenges and International Cooperation

Cybercrime often involves actors across multiple jurisdictions, making enforcement and prosecution more difficult. Each jurisdiction has different laws and approaches to cryptocurrency. International cooperation among law enforcement is necessary to pursue cybercriminals, yet coordinating across different regulatory frameworks remains challenging.¹⁹

¹⁸ Sanction Scanner, 2024. Everything You Should Know About Cryptocurrency Regulations In India

¹⁹ Freeman Law, 2022. Legal Issues Surrounding Cryptocurrency

Cybersecurity and Regulatory Compliance:

Cryptocurrency exchanges, wallets, and related infrastructure are prime targets for cybercrime, including hacking, phishing, and ransomware. Regulators may require firms to implement specific cybersecurity measures, but the fast-evolving nature of cyber threats and the technical complexity of blockchain technology mean that compliance can be challenging to enforce.

Taxation and Reporting Obligations

The tax treatment of cryptocurrency varies widely, from countries treating it as currency to others taxing it as a form of property. This variability creates difficulties in enforcement, as individuals and companies may evade taxes by moving funds across borders. Reporting obligations for cryptocurrency transactions can be hard to enforce due to the pseudonymous nature of many blockchain transactions and decentralized exchanges.

LEGAL ASPECT:

Prevention of Money Laundering Act 2002: Money laundering activities in India are regulated by this act and it also imposes obligations on entities dealing with cryptocurrencies. As per section 4 of this act includes punishment of imprisonment not less than 3 yrs and not more than 7 years and a fine of 5 lakh rupees.²⁰

Information Technology Act 2000 – Section 43 deals with unauthorised access to computer systems, which can encompass unauthorised access to crypto currency wallets or exchanges. Section 66 deals with the use of computer for illegal crypto currency transactions.²¹

Foreign Exchange Management Act: Unauthorized trading or remittance involving cryptocurrencies can be penalized under FEMA regulations²²

RECOMMENDATIONS:

- The standard legal framework can be framed to regulate cryptocurrency and to prevent cybercrimes.
- Public awareness campaigns can be conducted in order to educate consumers about

²⁰ Department of Economic Affairs, 2023. The Money Laundering Act

²¹ India Code. (2000). Information Technology Act, 2000

²² Vance, 2024. Understanding FEMA: Regulations, Objectives & Penalties

common scams, phishing tactics, hacking and secured crypto currency usage can reduce fraud.

- Governments can work with industry experts to develop and recommend standards for security.
- Law enforcement agencies should develop or invest in blockchain forensics tools to trace illicit transactions.
- Enforcing stricter penalties for cybercrimes related to cryptocurrency could deter potential criminals.

CONCLUSION:

Cryptocurrency has emerged as a transformative force in finance, enabling faster, decentralized and often anonymous transactions. However, these same qualities that make cryptocurrency appealing have also made it a preferred medium for various forms of cybercrime, including money laundering, ransomware and illegal trade on the dark web. While it offers legitimate financial innovation, its relatively unregulated and anonymous nature poses challenge for law enforcement and regulators worldwide. Despite the growing sophistication in tracing cryptocurrency transactions, cybercriminals continue to exploit technological and regulatory gaps to evade detection. The research highlights the urgent need for a balanced regulatory approach that protects user privacy while enhancing accountability. International cooperation, more advanced tracking technologies, and clear legal frameworks can help mitigate the misuse of cryptocurrencies in cybercrime. In conclusion, while cryptocurrencies are not inherently criminal, the ease with which they facilitate certain cybercrimes demands a proactive and coordinated response from governments, the tech community and financial regulators. Only by addressing these challenges, society can fully harness the potential of cryptocurrencies in a safe and responsible manner.

REFERENCES:

1. <https://www.simplilearn.com/relationship-between-cryptocurrency-and-cybercrime-article>
2. <https://www.researchgate.net/publication/352375203> Cryptocurrencies as facilitators of cybercrime
3. <https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking>
4. <https://www.researchgate.net/publication/331384975> Crypto Currencies and Cybe

rcrime

5. <https://www.sciencedirect.com/science/article/pii/S1057521924003715>
6. <https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-021-00163-8>
7. https://stars.library.ucf.edu/context/etd2023/article/1110/viewcontent/A_SYSTEMATIC_REVIEW_OF_CRYPTOCURRENCIES_USE_IN_CYBERCRIMES.pdf
8. https://www.researchgate.net/publication/323654794_A_First_Look_at_Browser-Based_Cryptojacking

