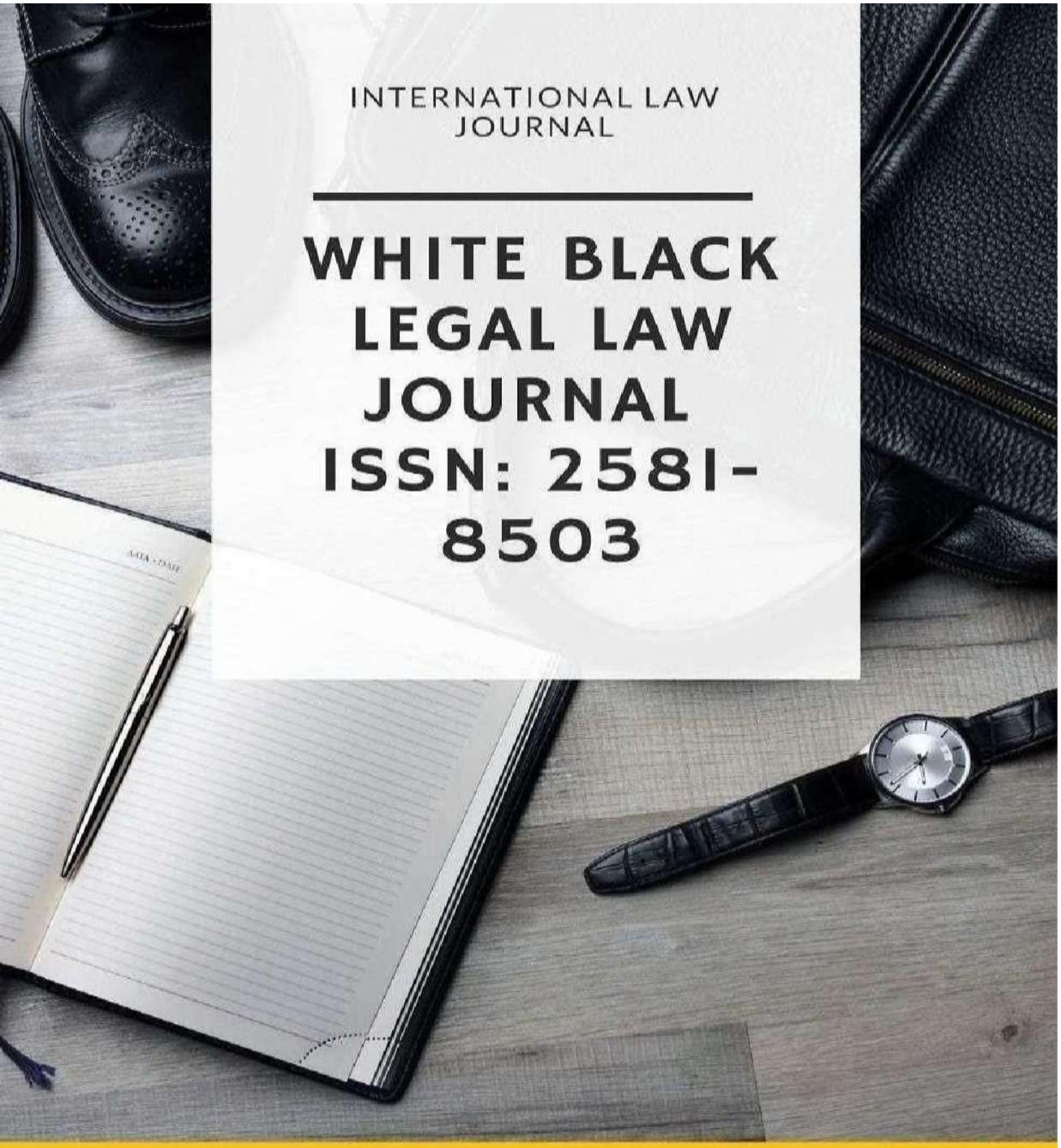

INTERNATIONAL LAW JOURNAL

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, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

A RESEARCH STUDY ON THE LEGAL IMPLICATION OF CRYPTO CURRENCY IN INDIA

AUTHORED BY - ANAND D
CO-AUTHOR - DR. J. KIRUBA SHARMILA
BBA LLB (Hons)
SCHOOL OF LAW, VISTAS

ABSTRACT

Cryptocurrency has surfaced as one of the most disruptive, financial and technological innovations of the twenty-first century. It stands as a challenge to the traditional, legal, regulatory, and monetary standards of the Indian economy. India's response towards crypto market has been very complex. It has evolved from early cautionary advisories to de facto prohibitions, and subsequently towards an ambiguous acceptance through heavy taxation and anti–money laundering regulations. India has understood that ignoring crypto won't make things any better, and instead of resisting, it has to slowly start taking measures.

The analysis begins by taking into account, the constitutional framework, throwing light on Article 19(1)(g) and also reviewing the Supreme Court's landmark judgment in its Internet Mobile Association of India vs Reserve Bank of India (2020) case. The court slashed down the RBI's 2018 outright ban as unreasonable, while emphasising the authenticity of a balanced and finely tuned regulation. It further proceeds by examining how the existing legislations, including the Income Tax Act, the Prevention of Money Laundering Act, Foreign Exchange Management Act, and the IPC, have adjusted to rectify cryptocurrency related fraudulent activities such as trading, terror funding, fraud, money laundering, hacking, and cross-border transfers.

By studying various case laws, enforcement actions, and institutional practices, the research also demonstrates as to how some Indian authorities might increasingly treat cryptocurrency as a property, in the absence of a uniform legal definition. At the same time, it also highlights the significant gaps like definitional ambiguity, a jurisdictional overlap among and between the

regulators, inadequate protection to the common man, data-protection issues and uncertainty and civil liability.

LEGAL IMPLICATIONS OF CRYPTOCURRENCY IN INDIA

The legal implications give a complete analysis for cryptocurrency law practice. It synthesises constitutional protections through article 19(1)(g), statutory architecture through sections 115BBH/194S, the criminal proceedings under IPC and its sections 403, 411 & 420 through Shailesh Bhatt case and also gives enforcement realities. This practical analysis tries to resolve the definitional confusions, provides precedent arguments, etc, trying to transform the constitutional theory into courtroom solutions while also giving a uniform crypto authority to captivate India's 2.3 lakh crore market under regulatory equilibrium.

1.1 CONSTITUTIONAL RIGHTS

ARTICLE 19:

The foundational constitutional principle in Indian cryptocurrency law emerges from Article 19(1)(g) of the Indian Constitution, which guarantees the right to practice any profession or carry on any occupation, trade, or business. This provision became central in the landmark Supreme Court judgment examined below.

In "Internet Mobile Association of India v. Reserve Bank of India" (2020), the Supreme Court held that the RBI's 2018 banking prohibition circular violated Article 19(1)(g) because it was a disproportionate restriction on the fundamental right to engage in cryptocurrency trading as a legitimate business activity. The Court acknowledged that while Article 19(6) permits reasonable restrictions on this right in the interest of general public, such restrictions must satisfy the proportionality doctrine.

The proportionality test applied by the Court required the RBI to demonstrate that: the restriction pursued legitimate objectives like financial stability, consumer protection, and prevention of money laundering; To prove that the means employed were appropriate to achieve that objective; the restriction were necessary; and also that, the benefits of the restriction outweighed the burden on fundamental rights.

The Court found that while the RBI's objectives were legitimate, the means—a complete banking prohibition—was disproportionate because the RBI failed to demonstrate that less restrictive means were ineffective. The RBI could regulate through KYC requirements, transaction monitoring, and licensing rather than complete prohibition.

PROPERTY RIGHTS AND INTANGIBLE ASSETS:

Cryptocurrencies raise complex questions regarding their classification as property under Indian law. The Constitution and various statutes recognize property rights as fundamental, though Article 300A grants the state power to acquire property for public purposes with compensation. The question of whether cryptocurrencies constitute "property" within the meaning of Indian law affects their legal treatability.

The Supreme Court in *Shailesh Bhatt case* (Ahmedabad Anti-Corruption Court, 2025) implicitly recognized Bitcoin as constituting "property" capable of being the subject of theft and extortion. When 14 individuals including police officers and a politician were sentenced to life imprisonment for kidnapping and extorting 34 Bitcoin (worth approximately Rs 2.5 crores at the time), the court treated Bitcoin as a valuable property capable of being dishonestly induced for delivery, thereby invoking IPC Section 420.

However, legislative definitions remain ambiguous. The Income Tax Act defines them as "Virtual Digital Assets," focusing on their characteristics as digital representations of value rather than their nature as property. This definitional ambiguity creates challenges for property rights, succession law, and family law applications.

CONSTITUTIONAL PRINCIPLES OF FEDERALISM:

A secondary constitutional issue concerns the division of powers between the central government and state governments. The Constitution allocates jurisdiction over currency and foreign exchange to the central government (Entry 36, List I), but assigns policing and criminal justice primarily to states (Entry 1, List II). Cryptocurrency's cross-border nature and digital form complicate this allocation.

The RBI, as the central bank, derives authority from the Reserve Bank of India Act, 1934 and the Banking Regulation Act, 1949. However, the Supreme Court in IAMAI v. RBI suggested that the RBI's authority over cryptocurrencies cannot rest solely on its role as currency regulator

when cryptocurrencies are not currencies. This jurisdictional question remains incompletely resolved, contributing to regulatory fragmentation.

1.2 STATUTORY LEGAL FRAMEWORK

INCOME TAX ACT:

The Union Budget 2022 introduced the most comprehensive statutory regulation of cryptocurrencies through two provisions in the Finance Act, 2022, effective April 1, 2023.

Section 115BBH provides: "Notwithstanding anything in this Act, where income is earned from the transfer of any virtual digital asset, such income shall be taxed at the rate of thirty per cent."

This provision establishes three critical rules:

First, Uniform Tax Rate: The 30 percent flat rate applies regardless of the individual's income tax slab, investment duration, or whether the income derives from business or investment activities. This represents a departure from the principle of progressive taxation embedded in Indian income tax law. A salaried employee in the 5 percent slab and a high-net-worth individual both pay 30 percent on cryptocurrency gains.

Second, No Loss Set-off: The statute expressly prohibits offsetting losses from virtual digital assets against gains from the same asset or other income sources. If an investor incurs a loss of Rs 1 lakh on Bitcoin while gaining Rs 2 lakhs on Ethereum, they cannot net the loss against the gain. This violates the general principle of loss adjustment in Indian tax law and creates potential tax inefficiency.

Third, Limited Deductions: Only the cost of acquisition is deductible. No other deductions, rebates, or exemptions apply. This prevents claiming losses on mining operations, transaction costs, exchange fees, or consulting fees.

The statutory basis for these provisions lies in the government's characterization of cryptocurrency transactions as generating "income from transfer of virtual digital asset." This classification sidesteps the question of whether cryptocurrency constitutes property, business, or investment, instead creating a sui generis category with its own tax regime.

Section 194S: Imposes a 1 percent Tax Deducted at Source (TDS) on payments made for the transfer of virtual digital assets. The TDS is payable when; the transfer exceeds Rs 10,000 in a single transaction, or the aggregate of transfers exceeds Rs 50,000 in a financial year (with variations for specified persons). The TDS mechanism serves dual purposes: it creates a transaction-level audit trail for tax authorities and acts as a disclosure mechanism for tracking cryptocurrency activities.

PREVENTION OF MONEY LAUNDERING ACT:

The landmark development in cryptocurrency regulation occurred through the March 7, 2023 notification by the Ministry of Finance, which brought "Virtual Digital Assets" (VDAs) and their service providers within the scope of the PMLA. This notification recognized exchanges, custodians, and wallet providers as "reporting entities" under the PMLA regime.

The PMLA framework imposes obligations on VDASPs:

KYC Requirements: All VDASPs must verify the identity of customers using government-issued identification linked to Aadhaar (unique identity number). The requirement extends to beneficial owners and ultimate beneficial owners for corporate clients.

Record Maintenance: VDASPs must maintain records of: customer identification information, all transactions involving VDAs, beneficial ownership details, transaction dates, amounts, and counterparties. These records must be retained for a minimum of five years, enabling law enforcement to reconstruct transaction chains.

Suspicious Transaction Reporting: When a transaction or series of transactions raises suspicion of money laundering, terrorists financing, or other financial crimes, the VASP must submit a Suspicious Transaction Report (STR) to the Financial Intelligence Unit. The reporting obligation is triggered when transactions exhibit characteristics inconsistent with the customer's profile, involve jurisdictions designated as high-risk, or relate to persons on watchlists.

Travel Rule Compliance: Following FATF guidance, the government expects VDASPs to obtain and verify origination information for cross-border transfers of virtual assets and ensure the information reaches the beneficiary's VASP. India has incorporated this standard, though enforcement mechanisms remain nascent.

Non-compliance with PMLA obligations exposes VDASPs to criminal liability. Section 69 of the PMLA provides for imprisonment up to 7 years and fines for persons involved in money laundering. Additionally, Directors of non-compliant exchanges face personal liability. The practical implications became evident when the Enforcement Directorate seized approximately Rs 936 crore in cryptocurrency under PMLA provisions between 2023-2025, and major exchanges including Binance received penalties of Rs 18.82 crores for KYC non-compliance.

FOREIGN EXCHANGE MANAGEMENT ACT:

The Foreign Exchange Management Act presents complex implications for cross-border cryptocurrency transactions. While the FEMA does not explicitly address cryptocurrency. Regulatory interpretation has classified cryptocurrencies as "intangible movable property" or "goods" rather than as "currency" or "foreign exchange."

Classification Issues: The FEMA defines "currency" as any medium of exchange, including currency notes and other instruments authorized by the RBI. When the RBI issued a notification clarifying that it does not classify cryptocurrency as currency under FEMA, this definitional exclusion became crucial. Consequently, buying or selling cryptocurrency does not constitute buying or selling foreign currency.

However, Section 2(h) of FEMA defines "foreign exchange" inclusively as foreign currency, foreign security, foreign exchange permits, and any other instrument representing foreign assets. The interpretation of whether cryptocurrency qualifies as a "foreign exchange" remains contested.

Capital Account versus Current Account Transactions: When an Indian resident engages in cryptocurrency transactions with non-residents, the FEMA categorizes such transactions as either:

Current Account Transactions (permitted subject to reporting): These involve payment for goods, services, or transfers of value across borders. Purchasing cryptocurrency from a foreign exchange in return for rupee payment constitutes a current account transaction. Such transactions are permissible under FEMA regulations but require documentation and may require approval for amounts exceeding specified thresholds.

Capital Account Transactions (restricted): These involve transfer of financial assets or investments across borders. While capital account transactions are generally more restricted,

certain cryptocurrency transactions involving investment in foreign digital assets may qualify as permissible capital account transactions under specified regulations.

Reporting and Compliance: Indian residents holding cryptocurrency in foreign wallets or exchanges must disclose such holdings in Schedule FA (Foreign Assets) of the Income Tax Return. Failure to disclose foreign cryptocurrency holdings may trigger prosecution under the Black Money (Undisclosed Foreign Income and Assets) Act, 2015, which provides for imprisonment up to 10 years and penalties up to 120 percent of the asset value.

Cr.P.C AND INFORMATION TECHNOLOGY ACT:

The Cr.P.C act 1973 provides the procedural framework for investigating and prosecuting cryptocurrency-related offences. Notably, Section 156(3) allows private persons to petition a Magistrate to direct police investigation when police decline to register a first information report (FIR). This provision has proven significant in cryptocurrency fraud cases where police initially hesitated to act.

The Information Technology Act, 2000 addresses computer-based crimes applicable to cryptocurrency. Section 43 provides for civil liability and damages for unauthorized access, introducing viruses, damaging systems, and stealing information. When hackers breach cryptocurrency exchange security systems, this section provides a civil remedy for damages. Section 66 criminalizes computer fraud with penalties up to 3 years imprisonment and Rs 3 lakhs fine. Unauthorized access to cryptocurrency wallets falls within this provision. Section 66F specifically criminalizes use of computer systems for terrorist financing, directly applicable when cryptocurrencies are used to fund terrorism.

1.3. CRIMINAL LAW FRAMEWORK: INDIAN PENAL CODE

SECTION 420:

The most frequently applied provision in cryptocurrency fraud cases is IPC Section 420, which provides: "Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security... shall be punished with imprisonment up to seven years and shall also be liable to fine."

Cryptocurrency fraud prosecutions typically allege that accused parties:

1. Made false representations regarding cryptocurrency value, returns, or legitimacy;
2. With knowledge of the falsity;
3. With intent to deceive;
4. Thereby induced victims to transfer cryptocurrency or fiat currency;
5. Causing loss to the victims.

In the landmark case of a Delhi-based cryptocurrency Ponzi scheme prosecuted in 2021, the accused operated a scheme promising 20-30 percent monthly returns. Over 61 victims lost Rs 2.5 crores. The court applied IPC Section 420 after finding that the accused knew cryptocurrency-based returns at promised levels were impossible and designed the scheme to attract victims' money, which was then misappropriated.

The Delhi High Court's July 2025 judgment refusing bail to Umesh Verma in the Pluto Exchange scam (Rs 50 crores) emphasized that "dealing in cryptocurrency has profound implications on the economy of our country by way of dissolution of recognised money into the dark, unknown, and untraceable money." This characterization illustrates judicial concern about cryptocurrency's role in facilitating fraud.

SECTION 403:

This provision applies when a person charged with property misappropriates it dishonestly. When cryptocurrency exchange executives misappropriate customer assets held in custody, this section applies. The Rs 378 crore Nebulu Technologies heist in Bengaluru (2024) involved allegations under this section when hackers, allegedly aided by a former employee, transferred cryptocurrency from the platform's hot wallets.

SECTION 411:

This provision criminalizes the receipt and possession of stolen cryptocurrency with knowledge of its unlawful origin. Given cryptocurrency's borderless nature and pseudonymous transactions, proving knowledge of unlawful origin presents significant evidentiary challenges. However, courts have begun considering blockchain transaction analysis and exchange know-your-customer records to establish the suspicious nature of receipt.

SECTION 379:

While traditional property theft involves physical objects, cryptocurrency theft exists in the digital realm. Courts have recognized that cryptocurrency can be the subject of theft under Section 379, treating the unauthorized taking of cryptocurrency from wallets or exchanges as constituting theft. This application has become relevant in exchange hacking cases and insider theft.

THE SHAILESH BHATT CASE:

The February 2025 Ahmedabad anti-corruption court judgment convicting 14 individuals, including 11 police officers and a BJP Member of the Legislative Assembly, for kidnapping and extorting 34 Bitcoin presents a significant precedent. The accused kidnapped Shailesh Bhatt on February 11, 2018, held him captive, beat him, and compelled him to liquidate 34 Bitcoin (worth approximately Rs 2.5 crores at the time) and transfer funds to the accused.

Applicable Offences: The court convicted the accused under: Section 364: Kidnapping for ransom, Section 363: Wrongful restraint, Section 307: Attempt to cause death, Section 392: Dacoity (robbery), IPC 420: Cheating (in falsely representing that they would release him), Section 120B: Criminal conspiracy, and Prevention of Corruption Act: Misconduct by public servants

The significance lies in the court's implicit recognition of Bitcoin as constituting property capable of being the subject of extortion and theft. By sentencing the accused to life imprisonment under general criminal law provisions applicable to property offences, the court treated cryptocurrency identically to traditional property for criminal law purposes.

CONSPIRACY AND ORGANIZED CRIME:

Cryptocurrency fraud frequently involves conspiracies among multiple actors—exchange operators, technical staff, promoters, and money laundering intermediaries. IPC Section 120B criminalizes conspiracy with punishment up to life imprisonment when the object is a serious offence. BitConnect scam prosecutions have extensively used conspiracy charges to prosecute the complex web of actors involved in the multi-level marketing scheme that defrauded investors of crores through false cryptocurrency returns promises.

1.4. REGULATORY INSTITUTIONS AND ENFORCEMENT

FINANCIAL INTELLIGENCE UNIT-INDIA (FIU-IND):

The FIU-IND serves as the nodal agency for anti-money laundering enforcement. Since March 2023, crypto exchanges and VDASPs must register with the FIU-IND and comply with anti-money laundering obligations. The FIU-IND operates under the PMLA and receives reports of suspicious transactions, high-value transactions, and cross-border fund flows.

By December 2025, the FIU-IND had: registered four offshore exchanges (Binance, Kraken, KuCoin, and Bybit) after they demonstrated compliance infrastructure; approved domestic exchanges including CoinDCX, CoinSwitch Kuber, and WazirX; had seized and frozen cryptocurrency worth Rs 936 crores in connection with money laundering investigations, filed criminal cases against non-registered exchanges and operators. The FIU-IND's registration regime operates as a de facto licensing system, distinguishing compliant exchanges from unregistered platforms.

ENFORCEMENT DIRECTORATE

The Enforcement Directorate, operating under the Department of Revenue, enforces PMLA and FEMA provisions. Since 2023, the ED has:

- Investigated approximately 44,000 cryptocurrency traders for black money violations;
- Attached or seized approximately Rs 936 crores in cryptocurrency;
- Filed cases against major exchanges for FEMA violations and failure to comply with KYC requirements;
- Coordinated with Interpol and foreign law enforcement for tracking proceeds of transnational cryptocurrency crimes.

The ED's role represents the government's shift from prohibition toward active enforcement and monitoring.

CYBERCRIME INVESTIGATION AGENCIES:

The Central Bureau of Investigation (CBI), Indian Computer Emergency Response Team (CERT-IN), and state cybercrime branches investigate cryptocurrency thefts and hacking. The WazirX hack (August 2024), involving the theft of Rs 2,000 crores worth of cryptocurrency, triggered a multi-agency investigation coordinating with the Financial Intelligence Unit, Interpol, and cryptocurrency intelligence firms like Chainalysis and Crystal Intelligence.