

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

A Critical Study of Asset Freezing Mechanisms and Tax Liability in Fraud-Affected Cryptocurrency Transactions in India

N SHANMUKHI PRAVALIKA* AND DR. JYOTIRMOY BANERJEE**

ABSTRACT

India has emerged as one of the world's largest cryptocurrency markets, with millions of investors participating in Virtual Digital Asset (VDA) transactions despite continuing regulatory uncertainty. At the same time, crypto-related frauds, hacking incidents, Ponzi schemes, and exchange failures have caused substantial financial losses to investors. Recent enforcement actions indicate a significant rise in regulatory intervention, with the Enforcement Directorate attaching crypto-linked assets worth hundreds of crores of rupees in money-laundering investigations, including attachments exceeding rupees 433 crore in the BitConnect-related case alone, while the Income Tax Department has intensified compliance measures by issuing more than 44,000 notices to crypto traders for non-reporting of VDA transactions and undisclosed income. Under Section 115BBH of the Income Tax Act, 1961, gains from VDAs are taxed at a flat rate of thirty per cent, accompanied by a one per cent tax deducted at source under Section 194S, while losses cannot be set off against other income or carried forward. Consequently, victims whose crypto assets have been frozen, seized, stolen, or rendered inaccessible through fraud may continue to face tax liabilities despite being deprived of any actual economic benefit. This paper critically examines the legal architecture governing asset-freezing mechanisms in India, including provisional attachment under the Prevention of Money Laundering Act, 2002, seizure powers under the Bharatiya Nagarik Suraksha Sanhita, 2023, and exchange-level restrictions imposed by Virtual Asset Service Providers. It analyses the disconnect between criminal enforcement measures and tax administration, demonstrating how overlapping regulatory actions can produce compounded financial hardship for fraud-affected investors. The paper further evaluates the socio-economic implications of this framework, including reduced investor confidence, under-reporting of cyber fraud, and diminished trust in digital financial markets. Drawing upon comparative regulatory developments under the European Union's Markets in Crypto-Assets Regulation, the paper proposes a coordinated victim-protection model incorporating tax suspension during

* Author is an LL.M. student at Amity Law School, Amity University, Bengaluru, India.

** Author is an Assistant Professor at Amity Law School, Amity University, Bengaluru, India.

asset-freeze proceedings, statutory recognition of fraud-related losses, and enhanced inter-agency coordination among the Enforcement Directorate, the Central Board of Direct Taxes, and cryptocurrency exchanges, with a view to a more equitable and investor-centric regulatory framework.

Keywords: *Cryptocurrency, Taxation, Asset freezing, Fraud, Compliance.*

I. INTRODUCTION

A. Background and context

The Indian cryptocurrency market has, within a single decade, travelled from a position of near-total regulatory neglect to one of the most actively policed corners of the financial system.¹ What began as a loosely supervised space for retail speculation has become a site of intense activity for two very different kinds of state actors: criminal investigators chasing the proceeds of fraud, and tax officers chasing undisclosed gains. Both actors increasingly target the same pool of assets, often the same individuals, and often arrive at strikingly different conclusions about what those assets represent: proceeds of crime on the one hand, taxable income on the other. The investor caught between these two characterisations is rarely in a position to argue with either.

This duality is not accidental. It reflects the way India has chosen to engage with virtual digital assets: not through a comprehensive regulatory statute that defines custody, licensing, consumer protection, and victim redress in one coherent instrument, but through a patchwork of fiscal provisions, anti-money-laundering amendments, and criminal-procedure tools² that were designed for an earlier, more conventional category of property. The *Finance Act, 2022* inserted Section 115BBH into the *Income Tax Act, 1961*, imposing a flat thirty per cent tax on gains from the transfer of virtual digital assets, alongside a one per cent tax deducted at source under Section 194S.³ Around the same set of years, the *Prevention of Money Laundering Act, 2002* was extended to bring Virtual Asset Service Providers within the definition of reporting entities, giving the Enforcement Directorate clear statutory footing to provisionally attach crypto holdings as proceeds of crime.⁴ Each of these moves was, on its own terms, defensible. Taken together, however, they have produced a regime in which a single set of digital tokens can

¹ *Internet & Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC 274 (India).

² *Internet & Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC 274 (India); The Prevention of Money Laundering Act, 2002, No. 15 of 2003, Acts of Parliament, 2003 (India).

³ The Finance Act, 2022, No. 6 of 2022, Acts of Parliament, 2022 (India) (inserting Sections 115BBH and 194S into the Income-tax Act, 1961).

⁴ Ministry of Finance, Notification No. S.O. 1072(E), Gazette of India, Extraordinary, pt. II, sec. 3(ii) (Mar. 7, 2023) (India).

simultaneously be the subject of a freezing order by one wing of government and a tax demand by another, with no formal bridge connecting the two proceedings.⁵

B. The Indian context

The scale of this overlap is no longer marginal. Enforcement data place the value of crypto-linked proceeds attached or seized by the Enforcement Directorate in the thousands of crores of rupees across a relatively short window, spanning cases ranging from cloned-exchange phishing operations to large multi-crore investment schemes disguised as forex or land-trading platforms.⁶ At the same time, the Income Tax Department has issued tens of thousands of notices to virtual-digital-asset holders under its data-matching exercises, comparing exchange-reported transaction data with individual tax filings, and has reported uncovering several hundred crores of rupees in undisclosed crypto-related income through search and seizure operations.⁷ The two enforcement streams are run by different ministries, rely on different statutory tests, and, critically, operate on different timelines. A criminal investigation into a fraudulent scheme may take years to conclude, during which an investor's frozen assets generate no liquidity, no access, and arguably no transfer in the sense contemplated by Section 115BBH. Yet the tax machinery, driven by automated data analytics that flag any recorded transfer on an exchange's books, does not necessarily pause for the criminal process to catch up.

The human consequence of this gap is visible in the pattern of recent cases. Victims of cloned-exchange scams, Telegram-based investment frauds, and fake decentralised-finance yield-farming schemes have reported losing access to wallets entirely, often with little realistic prospect of recovery once funds move to non-Indian exchanges or privacy-enhanced wallets. Where Indian exchanges are involved, freezing the destination address is sometimes possible, but recovery rates even in such cases remain modest. For these victims, a subsequent tax notice treating the fraudulent transfer of their holdings to a scammer's wallet as a taxable transfer generating notional gains, or treating their original investment as an asset whose loss cannot be set off against any other income, represents a second injury layered on top of the first.⁸

⁵ The Prevention of Money Laundering Act, 2002, No. 15 of 2003, §§ 5, 8, Acts of Parliament, 2003 (India); The Income-tax Act, 1961, No. 43 of 1961, §§ 115BBH, 194S, Acts of Parliament, 1961 (India).

⁶ Directorate of Enforcement, Ministry of Finance, Annual Report 2023-2024 (India); The Prevention of Money Laundering Act, 2002, No. 15 of 2003, §§ 5, 8, Acts of Parliament, 2003 (India).

⁷ Press Information Bureau, Gov't of India, *Income Tax Department Detects Undisclosed Income from Virtual Digital Assets Through Search and Survey Operations* (Dec. 2023); The Income-tax Act, 1961, No. 43 of 1961, §§ 115BBH, 194S, Acts of Parliament, 1961 (India).

⁸ The Finance Act, 2022, No. 6 of 2022, Acts of Parliament, 2022 (India) (inserting Section 115BBH into the Income-tax Act, 1961); The Prevention of Money Laundering Act, 2002, No. 15 of 2003, §§ 5, 8, Acts of Parliament, 2003 (India).

C. Rationale and scope

The existing academic and policy literature on Indian crypto regulation has tended to examine taxation, anti-money-laundering compliance, and consumer protection as separate silos. Tax scholarship focuses on the mechanics and rate structure of Section 115BBH; anti-money-laundering scholarship focuses on the adequacy of Know Your Customer and Travel Rule compliance by exchanges; and victim-protection commentary, where it exists at all, tends to be confined to practical guidance on what to do if scammed rather than systemic legal analysis. What is largely missing is a study that treats the asset-freezing function and the tax-collection function as two halves of a single governance problem, and that asks what happens, legally and practically, when both functions are activated against the same underlying asset pool in a fraud context.

This paper's central argument is that this represents a coordination failure with concrete distributive consequences. A regime that can simultaneously freeze an investor's assets as suspected proceeds of crime and tax that same investor on the notional gain represented by those frozen assets is not merely administratively untidy; it actively discourages victims from reporting fraud, complicates criminal prosecutions by giving victims an incentive to under-disclose their holdings, and risks converting the tax system into a secondary punishment for victims rather than a tool aimed at wrongdoers. The scope of this paper is accordingly confined to the Indian legal position, examining the attachment process under the *Prevention of Money Laundering Act, 2002*, the seizure and release provisions of the *Bharatiya Nagarik Suraksha Sanhita, 2023*, exchange-level freezing practices, and the operation of Section 115BBH and the penalty provisions of Section 270A, while drawing on the European Union's disclosure-oriented approach under the Markets in Crypto-Assets Regulation as a point of comparative reference for what a more integrated framework might look like.

D. Structure of the paper

The remainder of this paper proceeds as follows. The literature review examines electronic fraud, financial-system vulnerability, and the theoretical frameworks used to explain fraudulent conduct, drawing connections to the crypto-fraud context. The paper then sets out the objectives of the study and describes the research methodology. The principal analysis follows, examining the asset-freezing architecture, the tax-liability framework, the point of collision between the two, and comparative regulatory experience. The paper then distils the key findings, proposes a coordinated governance framework, and offers conclusions and recommendations for Indian policymakers, enforcement agencies, and affected investors.

II. LITERATURE REVIEW

A. Electronic fraud and financial-system vulnerability

The broader literature on electronic and cyber-enabled fraud provides a useful foundation for understanding crypto-fraud, even though much of it was developed in the context of conventional banking channels. Studies examining the role of deposit-taking institutions in financial development have generally emphasised that the credibility of any financial intermediary, whether a bank or a cryptocurrency exchange, depends on the strength of the regulatory and supervisory apparatus surrounding it, and that weaknesses in this apparatus have consequences that extend well beyond the immediate institution to affect public confidence in the financial system as a whole.⁹ This insight translates directly into the crypto context: the perceived legitimacy of licensed Virtual Asset Service Providers in India depends not only on their own internal controls but on the credibility of the wider enforcement and redress architecture that surrounds them.

The rapid expansion of electronic banking channels, while improving convenience and reducing operational costs, has simultaneously expanded the attack surface available to fraudsters. The same logic applies with even greater force to cryptocurrency platforms, which combine the pseudonymity of digital wallets with the irreversibility of blockchain-recorded transactions, a combination that makes both the commission of fraud and its subsequent investigation technically distinct from conventional banking fraud. Where a fraudulent bank transfer can sometimes be reversed or clawed back through the banking system's own settlement mechanisms, a fraudulent crypto transfer is, in the overwhelming majority of cases, final the moment it is confirmed on-chain. This finality shifts the entire burden of redress onto ex-post legal remedies such as asset freezing, which is precisely the mechanism this paper interrogates.¹⁰

B. Cyber-enabled fraud typologies and institutional costs

Research into specific fraud typologies, covering card-based fraud, point-of-sale fraud, mobile banking fraud, and internet banking fraud, has consistently found that such fraud imposes costs on the financial system well beyond the immediate loss to the victim. These costs include the expense of investigation, the administrative burden of compensation or reversal claims,

⁹ Ross Levine, *Financial Development and Economic Growth: Views and Agenda*, 35 J. ECON. LITERATURE 688 (1997).

¹⁰ Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, in PROC. 2013 CONF. ON INTERNET MEASUREMENT 127 (ACM 2013); The Prevention of Money Laundering Act, 2002, No. 15 of 2003, §§ 5, 8, Acts of Parliament, 2003 (India).

reputational damage to the institutions involved, and a broader erosion of customer trust in digital financial channels. Importantly, this literature has also found that the financial performance of affected institutions tends to suffer in proportion to the scale and sophistication of the fraud they are exposed to, with institutions experiencing slower revenue growth being disproportionately vulnerable to the financial consequences of fraud-related disputes and reversals.¹¹

When this framework is extended to cryptocurrency exchanges operating in India, a parallel set of institutional costs becomes visible. Licensed exchanges that are drawn into freezing orders, asset-tracing requests from the Enforcement Directorate, and Travel Rule compliance obligations bear significant operational costs that are distinct from, but related to, the costs borne directly by fraud victims. At the same time, the literature's finding that technological capability and proactive risk management can mitigate, though rarely eliminate, the financial consequences of fraud suggests that the policy response should not be confined to punitive measures against fraudsters alone, but should also strengthen the institutional capacity of exchanges and regulators to trace, freeze, and, where possible, restore assets before they move beyond the reach of Indian jurisdiction.¹²

C. Theoretical foundations: the fraud triangle and beyond

Donald Cressey's fraud triangle, which explains fraudulent conduct as the product of pressure, opportunity, and rationalisation operating together, continues to offer a useful lens for understanding why cryptocurrency has become such fertile ground for fraudulent schemes in India. The opportunity element of the triangle is significantly amplified in the crypto context: the technological novelty of blockchain transactions, the relative unfamiliarity of investigating officers with wallet tracing and exchange forensics until recently, and the cross-border nature of many platforms have together created an environment in which fraudulent schemes, whether cloned-exchange phishing operations, Telegram-based guaranteed-return groups, or fake decentralised-finance platforms, could operate with comparatively low detection risk for an extended period.

What the fraud triangle does not fully capture, however, is the secondary governance failure with which this paper is concerned: the way in which the state's own enforcement and tax

¹¹ M.L. Kanu & H.C. Okoroafor, *The Nature, Extent and Economic Impact of Fraud on Bank Deposits in Nigeria*, 4 INTERDISC. J. CONTEMP. RSCH. BUS. 253 (2013).

¹² Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* 15-25 (2021); The Prevention of Money Laundering Act, 2002, No. 15 of 2003, §§ 5, 8, Acts of Parliament, 2003 (India); Ministry of Finance, Notification No. S.O. 1072(E), Gazette of India, Extraordinary, pt. II, sec. 3(ii) (Mar. 7, 2023) (India).

machinery, once activated in response to a fraud, can itself become a source of hardship for the victim. This is not fraud in the Cressey sense, but it produces an analogous structural outcome. An individual who has already suffered a loss finds that the very systems designed to address that loss, criminal investigation and asset recovery on one side, tax administration on the other, operate independently of each other, leaving the victim to absorb the cost of their lack of coordination. A complete theoretical account of crypto-fraud governance in India therefore needs to extend beyond the motivations of the fraudster to the institutional design of the state's response.

D. Research gap

The literature reviewed above establishes, with reasonable consistency, that electronic and cyber-enabled fraud imposes significant costs on financial institutions and erodes public trust in digital financial channels, and that the fraud triangle remains a useful explanatory tool for why such fraud occurs. What remains comparatively underexplored, particularly within Indian legal scholarship, is the post-fraud regulatory experience of the victim, specifically the interaction between criminal asset-freezing mechanisms and the tax-liability framework applicable to virtual digital assets. Existing studies on Section 115BBH tend to treat tax compliance as a question for honest investors managing legitimate gains and losses, without addressing the position of an investor whose holdings have been fraudulently diverted, frozen by an investigating agency, or rendered permanently inaccessible. Equally, existing commentary on attachment under the Prevention of Money Laundering Act in crypto cases tends to focus on the agency's powers and enforcement statistics, without examining the downstream tax consequences for the very individuals whose assets have been attached or whose stolen funds have passed through a chain of wallets before recovery. This paper addresses that gap by treating asset freezing and tax liability as two interacting components of a single victim-facing governance problem.

III. OBJECTIVES OF THE STUDY

This research pursues two principal objectives.

The first objective is to critically examine the legal architecture governing the freezing, attachment, and seizure of cryptocurrency assets in India in cases involving fraud, including the powers exercised by the Enforcement Directorate under the *Prevention of Money Laundering Act, 2002*, the seizure and release mechanisms available under the *Bharatiya Nagarik Suraksha Sanhita, 2023*, and the practical role played by licensed Virtual Asset Service Providers in implementing such freezes.

The second objective is to analyse the tax-liability framework applicable to virtual digital assets under Section 115BBH of the *Income Tax Act, 1961*, with particular attention to its treatment of fraud-affected transactions, its rigid disallowance of loss set-off, and the resulting compounding effect on victims whose assets are simultaneously the subject of a freezing order and a tax demand, and, on this basis, to propose a coordinated framework that links asset-freezing proceedings to corresponding tax relief or suspension for genuine fraud victims.

IV. RESEARCH METHODOLOGY

This study adopts a doctrinal, analytical, and comparative methodology, relying primarily on secondary sources. The doctrinal component involves a systematic examination of the relevant statutory provisions, principally Sections 115BBH and 194S of the *Income Tax Act, 1961*,¹³ Sections 5, 8, and 17 of the *Prevention of Money Laundering Act, 2002*,¹⁴ and the seizure, attachment, and release provisions of the *Bharatiya Nagarik Suraksha Sanhita, 2023*,¹⁵ alongside reported judicial and tribunal decisions bearing on the taxation of virtual digital assets and the release of attached property.¹⁶

The analytical component involves a conceptual mapping exercise, tracing the procedural lifecycle of a hypothetical fraud-affected crypto transaction from the point of fraudulent diversion through to potential tax assessment, in order to identify the specific points at which the asset-freezing track and the tax-liability track intersect, diverge, or fail to communicate with each other.¹⁷ This mapping is informed by recent enforcement data drawn from official statements, parliamentary replies, and reported enforcement actions,¹⁸ which together provide a quantitative picture of the scale of both attachments under the Prevention of Money Laundering Act and Income Tax Department notices in the virtual-digital-asset space.

The comparative component places the Indian position alongside the European Union's Markets in Crypto-Assets Regulation,¹⁹ which, while not specifically designed as a victim-protection instrument, incorporates disclosure and consumer-protection obligations on crypto-asset service providers that offer a useful point of reference for thinking about how an Indian framework might better integrate victim identification into both the freezing and the tax-assessment

¹³ The Income-tax Act, 1961, No. 43 of 1961, §§ 115BBH, 194S, Acts of Parliament, 1961 (India).

¹⁴ The Prevention of Money Laundering Act, 2002, No. 15 of 2003, §§ 5, 8, 17, Acts of Parliament, 2003 (India).

¹⁵ The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, §§ 106-108, 497-503, Acts of Parliament, 2023 (India).

¹⁶ See generally decisions of the Income Tax Appellate Tribunal concerning virtual digital assets.

¹⁷ See generally H.L.A. Hart & Tony Honoré, *Causation in the Law* (2d ed. 1985).

¹⁸ Directorate of Enforcement, Ministry of Finance, Annual Report 2023-2024 (India); Central Board of Direct Taxes, Press Releases on Virtual Digital Assets (2022-2024).

¹⁹ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, 2023 O.J. (L 150) 40.

processes. Source materials include the *Income Tax Act, 1961* and the *Finance Act, 2022*; the *Prevention of Money Laundering Act, 2002*; the *Bharatiya Nagarik Suraksha Sanhita, 2023*; reported decisions of the Income Tax Appellate Tribunal and the High Courts on virtual-digital-asset taxation; enforcement statements and parliamentary replies concerning Enforcement Directorate and Central Board of Direct Taxes action in the crypto sector; and Regulation (EU) 2023/1114 on Markets in Crypto-Assets.²⁰

V. ANALYSIS

A. The architecture of asset freezing in crypto-fraud cases

When a cryptocurrency-related fraud is reported in India, the freezing of assets connected to the fraud can occur through at least three overlapping but procedurally distinct routes, each carrying its own consequences for the eventual position of the victim.

The first and most prominent route is provisional attachment under the *Prevention of Money Laundering Act, 2002*. Where the Enforcement Directorate has reason to believe that a person is in possession of proceeds of crime, a term that, following amendments bringing Virtual Asset Service Providers within the reporting framework of the Act, has been interpreted to extend to cryptocurrency holdings traceable to a predicate offence such as cheating or criminal conspiracy, it may provisionally attach such property for a period that can subsequently be confirmed by the Adjudicating Authority. Recent enforcement action illustrates the scale at which this power is now exercised: attachments running into thousands of crores of rupees have been made in large multi-jurisdictional schemes, while smaller but still substantial attachments running into single-digit or low double-digit crores have been made in more localised investment-fraud cases involving a handful of victims. In one such matter, the Enforcement Directorate's Chandigarh Zonal Office provisionally attached movable and immovable property together with cryptocurrency holdings, in a scheme that had combined fraudulent land-sale promises with assurances of high crypto returns affecting a relatively small group of investors.²¹ The attachment in such cases is not, in the first instance, framed as a remedy for the victims; it is framed as a seizure of proceeds of crime from the accused, with the victims' restitution being, at best, a downstream consequence contingent on confiscation proceedings and a subsequent claim process.²²

²⁰ The Finance Act, 2022, No. 6 of 2022, Acts of Parliament, 2022 (India); Regulation (EU) 2023/1114, 2023 O.J. (L 150) 40.

²¹ Directorate of Enforcement, Gov't of India, *ED, Chandigarh Zonal Office Provisionally Attaches Properties Including Cryptocurrencies in Fraud Case*, Press Release (2024).

²² The Prevention of Money Laundering Act, 2002, No. 15 of 2003, §§ 5, 8, Acts of Parliament, 2003 (India); *Vijay Madanlal Choudhary v. Union of India*, (2022) 10 SCC 386 (India).

The second route operates through the criminal-procedure framework now governed by the *Bharatiya Nagarik Suraksha Sanhita, 2023*, which succeeded the *Code of Criminal Procedure, 1973*.²³ Where property, including a cryptocurrency wallet or the balance held with an exchange, is alleged to be connected with a cognizable offence, investigating police officers may seize such property, and an aggrieved person, including a victim claiming ownership of the frozen assets, may approach the jurisdictional Magistrate for release of the property on establishing a legitimate claim. This route is procedurally distinct from attachment under the Prevention of Money Laundering Act and is often the first mechanism activated when a victim files a First Information Report, particularly in smaller-value cases that do not immediately attract Enforcement Directorate attention.²⁴ The practical difficulty with this route, however, is that the Magistrate's power to release property is discretionary and is typically exercised only after the investigating agency has had an opportunity to examine whether the property in question is itself tainted, a determination that, in a fraud case, frequently requires distinguishing between the fraudster's own assets and the diverted assets of the victim, a distinction that blockchain's pseudonymous and commingled transaction patterns can make genuinely difficult to draw.

The third route operates not through any court or tribunal order at all, but through the internal compliance procedures of licensed Virtual Asset Service Providers. Where an exchange identifies, whether through its own monitoring, a law-enforcement request, or a victim's complaint, that a wallet on its platform has received funds traceable to a reported fraud, it may freeze that wallet's balance pending further instructions, independent of any formal attachment order.²⁵ This route has produced some of the more encouraging recovery outcomes for victims, particularly where the destination wallet remains on an Indian exchange and the freeze is implemented quickly; reported recovery rates in such cases, while still modest in absolute terms, have been markedly higher than in cases where funds were moved promptly to wallets outside Indian exchange custody, where recovery rates have been reported in the low single digits. The speed of this exchange-level freeze is therefore often the single most consequential variable determining whether a victim recovers any part of their funds at all, far more consequential, in practical terms, than the eventual outcome of either the attachment proceedings or the criminal seizure process, both of which tend to operate on a timescale of months or years.²⁶

²³ The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, Acts of Parliament, 2023 (India); The Code of Criminal Procedure, 1973, No. 2 of 1974, Acts of Parliament, 1974 (India).

²⁴ The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, §§ 106-108, 497-503, Acts of Parliament, 2023 (India).

²⁵ Financial Intelligence Unit-India, Ministry of Finance, *Anti-Money Laundering and Counter Financing of Terrorism Guidelines for Reporting Entities* (2023).

²⁶ Financial Action Task Force, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (2024).

What unites all three routes is that none of them, in its present form, automatically triggers any corresponding notification to, or adjustment of, the victim's tax position.²⁷ An asset that has been provisionally attached as proceeds of crime, seized under the *Bharatiya Nagarik Suraksha Sanhita* pending a Magistrate's order, or frozen at the exchange level following a fraud complaint remains, from the perspective of the Income Tax Department's data-matching systems, simply a recorded transfer on the exchange's books, indistinguishable from a voluntary sale. The freezing order and the tax record exist in entirely separate informational silos.

B. Tax liability of fraud-affected investors

The tax treatment of virtual digital assets in India is governed principally by Section 115BBH of the *Income Tax Act, 1961*, inserted by the *Finance Act, 2022* with effect from the assessment year 2023-24.²⁸ The provision imposes a flat thirty per cent tax, together with applicable surcharge and a four per cent cess, on income arising from the transfer of any virtual digital asset, a category broadly defined to capture cryptocurrencies, non-fungible tokens, and similar digital representations of value. The provision is unusually severe in two respects that are of direct relevance to fraud victims.

First, Section 115BBH permits a deduction only for the cost of acquisition of the asset; no other expenditure, including, on at least one reading, the gas fees and brokerage charges incurred in acquiring or transferring the asset, is deductible,²⁹ although it is arguable that, on a purposive reading of Section 115BBH, brokerage and network transaction fees directly attributable to acquiring or transferring the asset should be treated as forming part of the cost of acquisition, even if ancillary platform subscription charges do not. More significantly for present purposes, the provision contains no exception, exemption, or special treatment for a transfer that occurs as a result of fraud, theft, or unauthorised access.³⁰ If a victim's wallet is drained by a phishing attack that mimics a legitimate exchange's interface, the on-chain record will show a transfer of value from the victim's wallet to the fraudster's wallet, a transfer that, read literally, falls within the scope of the charging language of Section 115BBH, even though the victim received no consideration whatsoever and exercised no voluntary disposition over the asset.

Second, and compounding the first point, Section 115BBH expressly disallows the set-off of any loss arising from virtual-digital-asset transactions against any other head of income, and

²⁷ The Income-tax Act, 1961, No. 43 of 1961, §§ 115BBH, 194S, Acts of Parliament, 1961 (India); The Finance Act, 2022, No. 6 of 2022, Acts of Parliament, 2022 (India).

²⁸ The Finance Act, 2022, No. 6 of 2022, Acts of Parliament, 2022 (India); The Income-tax Act, 1961, No. 43 of 1961, § 115BBH, Acts of Parliament, 1961 (India).

²⁹ The Income-tax Act, 1961, No. 43 of 1961, §§ 2(47A), 115BBH, Acts of Parliament, 1961 (India).

³⁰ The Income-tax Act, 1961, No. 43 of 1961, § 115BBH, Acts of Parliament, 1961 (India).

prohibits the carry-forward of such losses to subsequent assessment years. On the plain language of the provision, this loss-disallowance rule applies with full rigour regardless of the circumstances in which the loss arose, including circumstances of fraud, theft, or unauthorised access, since the statute draws no distinction based on how the loss was occasioned. The practical upshot is that an investor who, for example, purchased virtual digital assets for ten lakh rupees and subsequently had those assets stolen through a fraudulent scheme has, from the tax department's perspective, no loss to claim: the cost of acquisition simply vanishes from the investor's tax position without generating any deduction, while any recorded transfer connected to the fraud, whether the original fraudulent transfer to the scammer or a subsequent movement of the same assets through intermediate wallets before recovery proceedings begin, may itself attract scrutiny as a taxable event.³¹

The enforcement data bear out the scale at which this scrutiny now occurs.³² The Income Tax Department's data-analytics-driven NUDGE campaigns, built on matching Virtual Asset Service Providers' tax-deducted-at-source filings against individual income tax returns, have resulted in tens of thousands of notices being issued to virtual-digital-asset holders,³³ with the Central Board of Direct Taxes reporting the discovery of several hundred crores of rupees in undisclosed income through associated search and seizure operations, and total crypto-related crime proceeds seized by the Enforcement Directorate running into thousands of crores of rupees across a comparable period. Within this very large pool of flagged transactions, there is, at present, no mechanism by which the tax department's automated systems distinguish a transaction that represents a genuine, voluntary disposal of an asset from one that represents the involuntary, fraudulent diversion of an asset to a third party. Both are recorded, on the relevant exchange's books, in functionally identical terms.³⁴

C. The collision point: frozen assets and tax demands

The intersection of these two tracks, asset freezing on one side and tax assessment on the other, produces what this paper terms the collision point, and it is here that the practical injustice facing fraud victims becomes most visible.³⁵

³¹ The Income-tax Act, 1961, No. 43 of 1961, § 115BBH(2)(b), Acts of Parliament, 1961 (India); Nischal Shetty & Avinash Shekhar, *Everything You Wanted to Know About Cryptocurrency Taxation in India* (2022).

³² Central Board of Direct Taxes, Ministry of Finance, Gov't of India, Annual Report 2023-24.

³³ Central Board of Direct Taxes, Ministry of Finance, Gov't of India, *Press Release on VDA Compliance and NUDGE Campaign* (2024).

³⁴ Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Oct. 2021).

³⁵ The Income-tax Act, 1961, No. 43 of 1961, § 115BBH, Acts of Parliament, 1961 (India); The Prevention of Money Laundering Act, 2002, No. 15 of 2003, §§ 5, 8, Acts of Parliament, 2003 (India).

Consider a representative scenario drawn from the pattern visible in reported cases. An investor deposits funds with what appears to be a legitimate trading platform, promoted through a Telegram group promising high monthly returns. The platform operates for a period, during which the investor's holdings, as displayed on the platform's interface, appear to grow substantially. The platform then ceases operations abruptly, the administrator becomes unreachable, and the investor's wallet is found to be empty, the underlying tokens having been moved, often through a chain of intermediate wallets, to addresses outside the investor's control.³⁶ The investor files a complaint, and, if the case attracts sufficient attention, an investigation begins, potentially leading to a provisional attachment of whatever assets connected to the scheme can still be traced and frozen, whether held by the operator or sitting at an identifiable destination address on a licensed exchange.³⁷

At this point, two things can happen on the tax side, neither of which is presently addressed by any statutory carve-out.³⁸ First, if the investor's original deposit is treated, for tax purposes, as having been transferred at the moment it left the investor's wallet for the fraudulent platform's wallet, even though the investor received nothing of value in return and was the victim of deception, the investor may face a tax demand on a notional gain computed by reference to the value of the asset at the time of that transfer, with no corresponding ability to claim the subsequent total loss of the asset as an offsetting deduction.³⁹ Second, and somewhat perversely, if the investigating agency's attachment proceedings eventually result in some portion of the diverted assets being formally confiscated and credited toward victim restitution, a process that, even when successful, can take years, any value eventually received by the victim through that restitution process could itself, on a literal reading of the current framework, be treated as a fresh transfer generating a fresh tax event, computed without any reference to the investor's original cost of acquisition of the assets that were stolen in the first place, since the chain of custody between the original asset and the restituted value is rarely preserved in a form that the tax system recognises.

The result is a scenario in which an investor can be, first, defrauded of their original investment; second, assessed to tax on a notional gain arising from the fraudulent transfer itself; third, denied any deduction for the resulting loss; and, fourth, potentially assessed to tax again on any eventual, partial restitution recovered years later through a wholly separate enforcement

³⁶ *Id.*

³⁷ The Prevention of Money Laundering Act, 2002, No. 15 of 2003, §§ 5, 8, Acts of Parliament, 2003 (India); Directorate of Enforcement, Ministry of Finance, Gov't of India, Annual Report 2023-24.

³⁸ The Income-tax Act, 1961, No. 43 of 1961, § 115BBH, Acts of Parliament, 1961 (India).

³⁹ *Id.* § 115BBH(2); The Finance Act, 2022, No. 6 of 2022, Acts of Parliament, 2022 (India).

process, all without any of the four stages communicating with, or being aware of, the others.⁴⁰ Each stage, considered in isolation, may be a faithful application of the relevant statute. Considered together, they amount to a cumulative burden on the victim that bears no relationship to any wrongdoing on the victim's part, and that, if widely understood, would rationally deter victims from reporting fraud at all, since a report that triggers an Enforcement Directorate investigation also, indirectly, increases the visibility of the victim's transaction history to the very data-matching systems that generate Section 115BBH notices.

It is worth noting, too, that the recovery rates reported in practice, ranging from as low as around five per cent in cases involving seed-phishing where tracing through Indian exchanges is limited, to figures in the range of twelve to eighteen per cent in cases where an Indian exchange could freeze a destination address relatively quickly, to somewhat higher figures of around thirty-five per cent where victims used rapid-reporting channels, mean that the great majority of the value an investor originally committed is, in most cases, never recovered at all.⁴¹ Against this backdrop, a tax framework that treats the entire original investment as a sunk cost generating no deductible loss, while potentially treating the fraudulent diversion itself as a taxable event, imposes a burden that is disproportionate not merely in principle but in the overwhelming majority of actual outcomes.

D. Comparative regulatory models

The European Union's Markets in Crypto-Assets Regulation, while primarily a licensing and market-conduct instrument rather than a victim-protection statute in the narrow sense, offers a useful comparative reference point precisely because of the disclosure architecture it imposes on crypto-asset service providers.⁴² Under that framework, service providers face structured obligations to maintain records of client holdings and transaction histories in a form that is readily available to both the firm and, where lawfully required, to regulators, obligations that, while designed primarily for market-integrity and prudential purposes, have the incidental effect of making it considerably easier to reconstruct the provenance of a given holding when a dispute, fraud allegation, or asset-freezing request arises.⁴³

⁴⁰ The Income-tax Act, 1961, No. 43 of 1961, § 115BBH(2)(b), Acts of Parliament, 1961 (India); The Prevention of Money Laundering Act, 2002, No. 15 of 2003, §§ 5, 8, Acts of Parliament, 2003 (India).

⁴¹ Chainalysis, *The Chainalysis Crypto Crime Report 2025* (2025); TRM Labs, *Crypto Crime Report* (2024); Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Oct. 2021).

⁴² Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, and Amending Regulations (EU) No. 1093/2010, (EU) No. 1095/2010 and (EU) No. 1096/2010 and Directives 2013/36/EU and (EU) 2019/1937, 2023 O.J. (L 150) 40 [hereinafter MiCA Regulation].

⁴³ MiCA Regulation, *supra* note 42, arts. 66-68, 75; European Securities and Markets Authority, *Final Report on Guidelines under the Markets in Crypto-Assets Regulation* (2024).

India's regulatory trajectory has, by contrast, developed each strand of oversight, taxation, anti-money laundering, and, to the extent it exists at all, consumer protection, through separate legislative instruments enacted at different times for different purposes, without any unifying record-keeping or disclosure standard that would allow a victim's transaction history to be reconstructed once for the purposes of both an asset-freezing proceeding and a tax assessment.⁴⁴

The practical consequence is duplication: a victim cooperating with an Enforcement Directorate investigation into the fraud they suffered may be required to produce essentially the same transaction records, separately, to substantiate a claim for relief from a Section 115BBH notice, assuming, optimistically, that any such claim for relief is even cognisable under the present statutory language, which, as discussed above, it largely is not.⁴⁵

A further point of comparative interest lies in the treatment of cost-of-acquisition disputes.⁴⁶ It is arguable that, on a purposive reading of Section 115BBH, brokerage and network transaction fees directly attributable to a virtual-digital-asset transaction fall within the cost of acquisition even though ancillary platform subscription charges do not; interpreting the cost-of-acquisition concept in a manner that reflects the practical economics of crypto transactions, rather than adopting a narrow literal reading, is more consistent with the settled principle that a charging provision must be read together with its computational machinery. A willingness to engage with the practical realities of crypto transactions in this way suggests that there may be scope, through either judicial interpretation or, preferably, legislative amendment, for a similarly practical reading of what constitutes a transfer for the purposes of Section 115BBH, one that would exclude involuntary, fraudulent diversions of assets from the scope of the charging provision in the first instance, rather than requiring victims to seek relief only after a notional tax liability has already crystallised.⁴⁷

⁴⁴ The Income-tax Act, 1961, No. 43 of 1961, § 115BBH, Acts of Parliament, 1961 (India); The Prevention of Money Laundering Act, 2002, No. 15 of 2003, Acts of Parliament, 2003 (India); The Finance Act, 2022, No. 6 of 2022, Acts of Parliament, 2022 (India); Ministry of Finance, Notification No. S.O. 1072(E) (Mar. 7, 2023) (India) (bringing Virtual Digital Asset Service Providers within the reporting framework under the Prevention of Money Laundering Act).

⁴⁵ The Income-tax Act, 1961, No. 43 of 1961, § 115BBH(2), Acts of Parliament, 1961 (India); Directorate of Enforcement, Ministry of Finance, Gov't of India, Annual Report 2023-24.

⁴⁶ The Income-tax Act, 1961, No. 43 of 1961, § 115BBH(2)(a), Acts of Parliament, 1961 (India).

⁴⁷ The Income-tax Act, 1961, No. 43 of 1961, §§ 2(47), 2(47A), 115BBH, Acts of Parliament, 1961 (India); *Commissioner of Income Tax v. B.C. Srinivasa Setty*, (1981) 2 SCC 460 (India) (emphasising that charging provisions must be interpreted in conjunction with computational provisions).

VI. KEY FINDINGS

First, asset freezing in Indian crypto-fraud cases operates through at least three procedurally distinct routes, provisional attachment under the Prevention of Money Laundering Act, seizure and release under the *Bharatiya Nagarik Suraksha Sanhita*, and exchange-level freezes, each with different timelines, different evidentiary thresholds, and markedly different practical outcomes for victims, with exchange-level freezes on Indian platforms offering the most realistic, though still limited, prospect of recovery.

Second, Section 115BBH of the *Income Tax Act, 1961* contains no statutory carve-out, exemption, or special procedure for transactions arising from fraud, theft, or unauthorised access, meaning that a fraudulent diversion of assets is, on a literal reading, capable of being treated as a taxable transfer while the resulting loss remains non-deductible and non-carry-forward under the same provision.

Third, the asset-freezing track and the tax-assessment track operate in entirely separate informational silos, with no mechanism by which a provisional attachment, a criminal seizure, or an exchange-level freeze automatically informs or pauses the Income Tax Department's data-matching and notice-issuance processes in respect of the same underlying transactions.

Fourth, the scale of both enforcement tracks has grown substantially and in parallel, with crypto-linked proceeds attached running into thousands of crores of rupees and tax notices issued in the tens of thousands, meaning that the population of individuals potentially exposed to the collision point identified in this paper is not a small or theoretical group, but a substantial and growing one.

Fifth, reported recovery rates for crypto-fraud victims remain low across most case typologies, meaning that the practical effect of the current tax framework's loss-disallowance rule, applied to fraud-affected transactions, is to convert what is already a near-total economic loss for the victim into a potential tax liability as well.

Sixth, comparative experience under the European Union's Markets in Crypto-Assets Regulation, and the incremental willingness of Indian courts to interpret cost-of-acquisition provisions in a manner that reflects the practical realities of crypto transactions, together suggest that a more integrated, victim-aware framework is both conceptually available and consistent with the direction in which Indian jurisprudence is already, cautiously, moving.

VII. A PROPOSED FRAMEWORK: THE VICTIM-COORDINATED ENFORCEMENT AND TAXATION MODEL

Building on the findings above, this paper proposes a Victim-Coordinated Enforcement and Taxation framework, structured around three linked mechanisms.

The first mechanism is a freeze-to-flag notification. Where the Enforcement Directorate issues a provisional attachment order, or a licensed Virtual Asset Service Provider implements an exchange-level freeze in response to a verified fraud complaint, a standardised notification should be transmitted through a secure inter-agency data channel to the Central Board of Direct Taxes, flagging the specific wallet addresses and transaction identifiers involved. This would not, by itself, alter any taxpayer's liability, but would ensure that automated data-matching systems are aware that a given transaction is the subject of an active fraud investigation before any notice is generated in respect of it.

The second mechanism is the suspension of assessment pending investigation. Where a transaction has been flagged under the first mechanism, any Section 115BBH assessment or notice referable to that specific transaction should be administratively suspended until the underlying criminal investigation reaches a defined milestone, for instance, the filing of a charge sheet confirming or rejecting the fraud allegation. This mirrors, in structure, existing principles under which assessment proceedings may be kept in abeyance pending the outcome of connected proceedings, and would prevent the situation, described above, in which a victim faces a tax demand on a transaction that the state's own investigating agency has independently identified as potentially fraudulent.

The third mechanism is statutory loss recognition for confirmed fraud victims. Where a criminal investigation concludes, whether through a charge sheet, a conviction, or a confirmed attachment order under the Prevention of Money Laundering Act, that a named individual was the victim of a fraudulent scheme involving virtual digital assets, that individual should be entitled to claim the cost of acquisition of the assets so lost as a recognised capital loss, available for set-off against other capital gains, including, but not limited to, other virtual-digital-asset gains, in the assessment year in which the fraud is confirmed. This would require a targeted amendment to Section 115BBH, carving out a narrow and evidentially anchored exception to the general loss-disallowance rule, an exception triggered only by an official finding of fraud, and therefore not available as a general avoidance route for ordinary trading losses.

Together, these three mechanisms are designed to ensure that the considerable enforcement capacity India has built up in respect of crypto-related crime, reflected in the scale of

attachments and prosecutions reported by the Enforcement Directorate, operates for victims as well as against fraudsters, rather than generating, as a side effect, a second wave of liability for the people the system is ostensibly protecting.

VIII. CONCLUSION AND RECOMMENDATIONS

India's response to cryptocurrency-related fraud has, on its own terms, become considerably more capable over a short period. Provisional attachments running into thousands of crores of rupees, high reported conviction rates for completed prosecutions, and an income tax data-matching apparatus capable of flagging tens of thousands of individual taxpayers all demonstrate that the state's capacity to detect both fraud and tax non-compliance in the virtual-digital-asset space has grown substantially. What has not grown at a comparable pace is the state's capacity to distinguish, within that detected population, between the wrongdoer and the wronged.

This paper has argued that the absence of any coordination between the asset-freezing architecture, operating through the *Prevention of Money Laundering Act*, the *Bharatiya Nagarik Suraksha Sanhita*, and exchange-level compliance practices, and the tax-liability architecture under Section 115BBH of the *Income Tax Act, 1961*, produces a collision point at which genuine fraud victims can find themselves facing tax demands on the very transactions through which they were defrauded, with no statutory recognition of their loss and no procedural mechanism to pause assessment pending the outcome of the investigation into their own victimisation. Given that reported recovery rates for crypto-fraud victims remain low across most case typologies, the practical effect of this gap is to compound, through the tax system, a loss that the criminal justice system has already been unable to fully remedy.

The recommendations arising from this analysis are addressed to three audiences.

For Indian policymakers, a targeted amendment to Section 115BBH should be introduced to recognise a narrow, evidentially anchored exception for confirmed fraud losses, modelled on the third mechanism proposed above. In parallel, the Central Board of Direct Taxes and the Enforcement Directorate should establish a standing data-sharing protocol, the freeze-to-flag mechanism proposed above, to ensure that transactions under active fraud investigation are not subjected to routine notice-generation processes designed for ordinary non-compliance.

For the Income Tax Appellate Tribunal and the higher judiciary, building on the incremental, practically grounded approach already visible in recent decisions concerning the cost-of-acquisition concept under Section 115BBH, courts and tribunals confronted with cases involving fraud-affected transactions should consider whether an involuntary, fraudulently

induced transfer falls within the charging language of Section 115BBH at all, rather than treating the question solely as one of deduction or loss set-off after liability has already been found to arise.

For licensed exchanges and Virtual Asset Service Providers, exchanges should treat the speed of their internal freeze-response process as a core consumer-protection metric, given the evidence that a promptly implemented exchange-level freeze represents the single most consequential factor in determining whether a victim recovers any part of their funds. Exchanges should also maintain transaction-history records in a form readily exportable for use in both criminal proceedings and any future tax-relief claim a victim may need to make, reducing the duplication of effort that currently falls on victims navigating both systems separately.

Cryptocurrency governance in India cannot be considered complete while its two principal enforcement arms, one aimed at recovering the proceeds of crime, the other at collecting tax on digital-asset transactions, continue to operate as though the population of persons affected by each were entirely distinct. In the great majority of fraud cases, they are not. A framework that recognises this overlap, and that is designed from the outset to ensure that enforcement against fraudsters does not translate into a second liability for their victims, would represent a meaningful and achievable step toward a digital-asset governance architecture that is not only effective but also just.

IX. BIBLIOGRAPHY

1. *Statutes and legislative materials*
2. The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, Acts of Parliament, 2023 (India).
3. The Code of Criminal Procedure, 1973, No. 2 of 1974, Acts of Parliament, 1974 (India).
4. The Finance Act, 2022, No. 6 of 2022, Acts of Parliament, 2022 (India).
5. The Income-tax Act, 1961, No. 43 of 1961, Acts of Parliament, 1961 (India).
6. The Prevention of Money Laundering Act, 2002, No. 15 of 2003, Acts of Parliament, 2003 (India).
7. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, and Amending Regulations (EU) No. 1093/2010, (EU) No. 1095/2010 and (EU) No. 1096/2010 and Directives 2013/36/EU and (EU) 2019/1937, 2023 O.J. (L 150) 40.

8. Ministry of Finance, Notification No. S.O. 1072(E), Gazette of India, Extraordinary, pt. II, sec. 3(ii) (Mar. 7, 2023) (India).
9. *Cases*
10. *Commissioner of Income Tax v. B.C. Srinivasa Setty*, (1981) 2 SCC 460 (India).
11. *Sunderbhai Ambalal Desai v. State of Gujarat*, (2002) 10 SCC 283 (India).
12. *Vijay Madanlal Choudhary v. Union of India*, (2022) 10 SCC 386 (India).
13. *Government reports and official publications*
14. Central Board of Direct Taxes, Ministry of Finance, Gov't of India, Annual Report 2023-24.
15. Central Board of Direct Taxes, Ministry of Finance, Gov't of India, Circular No. 13 of 2022: Guidelines for Removal of Difficulties Under Section 194S of the Income-tax Act, 1961 (June 22, 2022).
16. Central Board of Direct Taxes, Ministry of Finance, Gov't of India, Press Release on VDA Compliance and NUDGE Campaign (2024).
17. Directorate of Enforcement, Gov't of India, Annual Report 2023-24.
18. Directorate of Enforcement, Gov't of India, Frequently Asked Questions on the Prevention of Money Laundering Act (2023).
19. Directorate of Enforcement, Gov't of India, Press Release on Provisional Attachment of Properties Including Cryptocurrencies by the Chandigarh Zonal Office (2024).
20. Financial Intelligence Unit-India, Ministry of Finance, Anti-Money Laundering and Counter Financing of Terrorism Guidelines for Reporting Entities (2023).
21. European Securities and Markets Authority, Final Report on Guidelines under the Markets in Crypto-Assets Regulation (2024).
22. *International organisations and institutional reports*
23. Financial Action Task Force, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (2024).
24. Financial Action Task Force, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Oct. 2021).
25. Financial Action Task Force, Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (Sept. 2020).

26. Organisation for Economic Co-operation and Development, Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard (2022).
27. *Industry reports*
28. Chainalysis, The Chainalysis Crypto Crime Report 2025 (2025).
29. TRM Labs, Crypto Crime Report (2024).
30. *Books*
31. Nischal Shetty & Avinash Shekhar, Everything You Wanted to Know About Cryptocurrency Taxation in India (2022).
