IJHRL | FVADI-SPECIAL ISSUE- DECEMBER 2025 ISSN: 3107-5827 (ONLINE)

INTERNATIONAL JOURNAL OF

HUMAN RIGHTS AND LAW

PUBLISHED BY

HUMAN RIGHTS COUNCIL OF INDIA

Punjab & Haryana

A Peer Reviewed Bi-Annual Refereed E-Journal

Edited Volume / Special Issue

From the National Conference held on 14 December 2025

Future of Virtual Digital Assets in India, 2025 Legal, Regulatory and Economic Perspectives

Organiser:-

Pitambara Legal Associates, New Delhi

In Collaboration with

Human Rights Council of India (Punjab & Haryana)

Published in Association with

International Journal of Human Rights and Law

ISSN: 3107-5827 (Online)

Publication Year: 2026

Future of Virtual Digital Assets in India, 2025

Legal, Regulatory and Economic Perspectives

Cite this Publication as:

***Future of Virtual Digital Assets in India, 2025: Legal, Regulatory and Economic Perspectives*, Special Issue, International Journal of Human Rights and Law (2026).**

INTERNATIONAL JOURNAL OF
HUMAN RIGHTS AND LAW
ISSN: 3107-5827 (ONLINE)

International Journal of Human Rights and Law (IJHRL)

ISSN: 3107-5827 (Online)

The journal is part of the broader efforts by the *Human Rights Council of India (Punjab & Haryana),* which works on numerous initiatives aimed at promoting and protecting human rights.

This Special Issue is a curated academic volume containing selected, peer-reviewed papers presented at the National Conference on the Future of Virtual Digital Assets in India, 2025: Legal, Regulatory and Economic Perspectives, held on 14 December 2025 in an online mode.

The conference was organised by Pitambara Legal Associates, New Delhi, in collaboration with the Human Rights Council of India (Punjab & Haryana), and aimed at fostering legal, policy, and academic discourse on the evolving landscape of Virtual Digital Assets (VDAs) in India. The conference materials and publication plan identify the event, theme, organisers, and the associated publication opportunity with the International Journal of Human Rights and Law (ISSN: 3107-5827).

Published in Association with International Journal of Human Rights and Law
ISSN: 3107-5827 (Online)

Publication Year: 2026

International Journal of Human Rights and Law (ISSN: 3107-5827)
Human Rights Council of India (Punjab & Haryana)

Disclaimer

This publication is a bona fide work of the authors and editors. The International Journal of Human Rights and Law (ISSN: 3107-5827), along with its associates, bears no liability for the views and opinions expressed herein. The research material presented is the result of collective academic efforts based on existing data, sources, and references.

All due care has been taken to acknowledge and credit original sources, and no copyright infringement is intended. Any inadvertent errors or omissions are purely unintentional. The publisher and editors shall not be held responsible for any adverse consequences arising from the use or interpretation of the research contained in this publication.

Published by
International Journal of Human Rights and Law
ISSN: 3107-5827 (Online)
Human Rights Council of India (Punjab & Haryana)

In Collaboration with
Pitambara Legal Associates, New Delhi

Associated with
National Conference on *Future of Virtual Digital Assets in India, 2025*
(Legal, Regulatory and Economic Perspectives)
Date of Conference: 14 December 2025

Nature of Publication

This volume contains selected and peer-reviewed research papers presented during the conference and curated for publication in a Special Issue format. The conference brochure and concept note outlined the theme, objectives, and publication opportunity for selected papers in the International Journal of Human Rights and Law.

Theme of the Conference

Future of Virtual Digital Assets in India: Legal, Regulatory and Economic Perspectives

---

Objectives of the Conference

a. *To critically examine the evolving legal framework governing Virtual Digital Assets (VDAs) in India.*
b. *To analyse regulatory challenges and policy gaps in light of global best practices.*
c. *To explore the intersection of VDAs with financial systems, taxation, and economic governance.*
d. *To assess the implications of blockchain technologies on privacy, data protection, and human rights.*
e. *To encourage interdisciplinary dialogue among legal scholars, policymakers, industry experts, and researchers.*
f. *To provide a platform for emerging researchers to contribute to contemporary debates on digital asset regulation.*
g. *To identify pathways for a balanced and innovation-friendly regulatory ecosystem in India*

EDITORIAL NOTE

The legal and policy discourse surrounding Virtual Digital Assets (VDAs) has rapidly emerged as one of the most dynamic and consequential areas of contemporary legal scholarship. As India continues to evolve within the broader digital economy, questions relating to cryptocurrencies, blockchain systems, NFTs, tokenised assets, taxation, investor protection, regulatory governance, privacy, and cybersecurity have assumed increasing significance.

In this context, the National Conference on Future of Virtual Digital Assets in India, 2025: Legal, Regulatory and Economic Perspectives was conceived as an academic platform to foster critical engagement with the legal and economic implications of Virtual Digital Assets in India. The conference invited participation from students, academicians, legal researchers, professionals, and policy thinkers, and encouraged interdisciplinary scholarship on one of the most rapidly evolving domains of law and governance. The conference materials specifically framed the event around legal, regulatory, taxation, policy, and comparative issues concerning VDAs in India.

This Special Issue is the result of that academic initiative. It brings together a curated selection of research papers presented at the conference, chosen on the basis of:

- Originality of thought
- Relevance to the conference theme
- Analytical depth
- Research quality
- Contemporary legal significance

The papers included in this volume reflect a broad range of perspectives on Virtual Digital Assets, including regulatory ambiguity, comparative legal approaches, digital trust, taxation policy, cybersecurity, smart contracts, consumer protection, and the future of digital asset governance.

We hope this publication contributes meaningfully to the growing scholarship on law, technology, finance, and digital governance and serves as a useful academic resource for researchers, institutions, practitioners, and policymakers.

—Editorial Team; International Journal of Human Rights and Law; ISSN 3107-5827

FOREWORD

It gives us immense pleasure to present this Special Issue Volume containing selected research papers from the National Conference on Future of Virtual Digital Assets in India, 2025: Legal, Regulatory and Economic Perspectives.

The conference was organised with the objective of creating a meaningful platform for critical discussion on one of the most emerging and legally complex subjects of the present era — Virtual Digital Assets. The increasing relevance of digital finance, decentralized systems, tokenized assets, and blockchain-based transactions has generated important legal and policy concerns that require sustained academic and institutional engagement.

The quality of participation and the depth of the papers presented during the conference clearly demonstrated the growing interest among students and scholars in the intersection of law, regulation, technology, taxation, cybersecurity, and governance.

This publication has been conceptualised as a continuation of that academic effort. By compiling selected research papers into a Special Issue, we aim to preserve and promote the valuable scholarship presented at the conference and to provide a formal platform for emerging voices in this evolving field.

We extend our sincere gratitude to all speakers, moderators, authors, participants, reviewers, academic supporters, and collaborators who contributed to the success of the conference and this publication.

We hope this volume inspires further legal research and policy engagement on the future of Virtual Digital Assets in India.

Pitambara Legal Associates, New Delhi
Human Rights Council of India (Punjab & Haryana)

ABOUT THE CONFERENCE

The National Conference on "Future of Virtual Digital Assets in India 2025" was held virtually on 14 December 2025, organized by Pitambara Legal Associates, New Delhi, in collaboration with the Human Rights Council of India (Punjab & Haryana) and the International Journal of Human Rights and Law (IJHRL). The conference brought together scholars, legal practitioners, policymakers, and students to deliberate on the legal, regulatory, economic, and technological aspects of Virtual Digital Assets (VDAs) in India.

As India emerges as a major participant in the global digital economy, technologies such as cryptocurrencies, blockchain, smart contracts, NFTs, and tokenized financial ecosystems have begun to influence legal and regulatory frameworks in unprecedented ways. While these developments present opportunities for innovation, financial inclusion, and technological transformation, they also raise serious concerns relating to:

a. **Regulation and compliance**
b. **Taxation and financial governance**
c. **Consumer and investor protection**
d. **Privacy and data security**
e. **Cybercrime and digital fraud**
f. **Cross-border legal and policy implications**

The conference was designed to provide a platform for students, academicians, legal scholars, practitioners, and experts to engage with these emerging issues through academic research and critical discussion.

Inaugural Session

The conference commenced at 9:00 AM with a warm welcome address by Ms. Tanushri Kapur, Founder & Managing Partner, Pitambara Legal Associates. The Chief Guest, Dr. Ivneet Walia, Registrar of Rajiv Gandhi National University of Law, Punjab, followed with remarks, and the Guest of Honour, Dr. Suranjan Chakraborty, Civil Judge, Kolkata, and Chairman of the Legal & Research Cell at the Human Rights Council of India (Punjab & Haryana), highlighted the judicial perspective. The Keynote Address was delivered by Dr. Gaurav Gupta, Scientist F and

Director, Ministry of Electronics & Information Technology (MeitY), emphasizing the technological and policy dimensions of VDAs. The inaugural session concluded with a vote of thanks by Dr. Prithivi Raj, Assistant Professor, Birla Global University, Odisha, and Legal Advisor at the Human Rights Council of India (Punjab & Haryana), moderated by Ms. Pooja Ajay Talim, LL.B student, University of Mumbai.

Panel Discussion 1

From 10:00 AM to 12:00 PM, Panel Discussion 1 focused on *"VDAs: Legal, Taxation, Regulatory & Policy Issues"*. Chaired by Mr. Sandeep Jindal, Advocate-on-Record, Supreme Court of India, the session explored risks and challenges in the use of VDAs. The expert speaker, Mr. Rahul Dua, KYC/AML professional and Certified Cryptocurrency Investigator, discussed regulatory impacts on VDA service providers. Panelists Mr. Chetandeep Batra (Tech Lawyer & Data Protection Officer), Ms. Sunayan Bhat (Assistant Professor, Christ University), and Dr. Shilpa ML (Assistant Professor, Christ University) elaborated on cybersecurity, privacy, regulatory frameworks, and consumer protection. The discussion was moderated by Mr. Kartikey Shukla, B.A.LL.B student, Rajiv Gandhi National University of Law, Punjab.

Panel Discussion 2

From 12:00 PM to 2:00 PM, Panel Discussion 2 addressed *"Blockchain, Smart Contracts, ADR & VDA Intersections, Criminal Law & VDA"*. Moderated by Ms. Pratibha Gaur, B.A. LL.B (Hons.) student, Dr. Rajendra Prasad National Law University, Prayagraj, the session was chaired by Adv. Dr. Deepika Saini, Founder of the Institute for Alternative Dispute Resolution, who spoke on blockchain, digital identity, and data ownership. Mr. Gantav Gupta, Assistant Professor, NMIMS University, Chandigarh, analyzed intersections of VDAs and criminal law. The keynote was delivered by Ms. Subha Chugh, Lawyer and Consultant in Blockchain & AI, followed by Adv. Dr. Neha Pawade, Founder of Drishti Enterprises, who discussed comparative perspectives from global VDA regulations.

Paper Presentation Sessions

The first paper presentation session (3:00 PM – 5:00 PM) was chaired by Dr. Suranjan Chakraborty and co-chaired by Ms. Tanushri Kapur, with Ms. Ruchita S. Vishwakarma, University of Mumbai, as moderator, and an invited talk by Dr. Deepak Sharma, Assistant Professor & HoD Law, Dr. Rajendra Prasad National Law University, Prayagraj. The session

featured seven research papers covering consumer protection, blockchain legal frameworks, taxation, trust mechanisms, and cybersecurity in VDAs.

The second paper presentation session (also 3:00 PM – 5:00 PM) was chaired by Dr. Prithivi Raj and co-chaired by Ms. Chanda Yadav, with Ms. Sapna Singh, Tech Policy Lawyer, providing an invited talk. This session highlighted regulatory challenges, data privacy, and legal frameworks for VDAs, showcasing contributions from six emerging scholars.

Valedictory Session

The conference concluded with the valedictory session (5:00 PM – 6:00 PM). Adv. Gagan Gandhi, Managing Partner, Niti Nayaya Law Firm, addressed *Digital Arrest in Virtual Digital Assets Transactions*, and Adv. Ekta Deb, Cyber Crime & Data Privacy Lawyer, spoke on *Navigating VDA Security: Code vs. Compliance*. The Best Paper Presentation awards were announced, followed by a vote of thanks by Dr. Arjun, Joint Secretary, Human Rights Council of India (Punjab & Haryana), with moderation by Ms. Ruchita S. Vishwakarma.

Outcome and Significance

The conference provided a comprehensive platform for dialogue on the rapidly evolving landscape of Virtual Digital Assets in India, integrating academic research, practical insights, and policy perspectives. Participants engaged in critical discussions on consumer protection, cybersecurity, taxation, dispute resolution, blockchain governance, and comparative international frameworks, fostering collaboration between legal scholars, practitioners, and policymakers.

IJHRL | FVADI-Special Issue- December 2025

Sr. No	Title	Page No.
1.	**CRYPTOCURRENCY TAXATION: WHAT INDIA CAN LEARN FROM SINGAPORE** ***Shiv Ratan Arora and Gitanjali Diwakar***	01-13
2.	**DIGITAL ASSETS AND THE LAW: AN INDIAN PERSPECTIVE WITH COMPARATIVE INSIGHTS FROM THE US AND UAE** ***Tassaduq Hussain***	14-25
3.	**BALANCING INNOVATION AND PROTECTION: A CRITICAL EXAMINATION OF INDIA'S LEGAL FRAMEWORK GOVERNING CYBERSECURITY AND DATA PRIVACY IN VIRTUAL DIGITAL ASSET TRANSACTIONS** ***Prishima K and N. Prabhavathi***	26-34
4.	**CRYPTO CONSUMER PROTECTION IN INDIA: EVALUATING REGULATORY GAPS IN MISLEADING PROMOTIONS, EXCHANGE FAILURES, AND GLOBAL BEST PRACTICES** ***Karan Gupta and Om Chopra***	35-44

CRYPTOCURRENCY TAXATION: WHAT INDIA CAN LEARN FROM SINGAPORE

Shiv Ratan Arora
Advocate
High Court of Allahabad

Gitanjali Diwakar
Advocate
High Court of Madras

Abstract

The recent judgment of the High Court of Madras has altered one's perceptions surrounding cryptocurrency in India. While some might deem it to be a step towards clarity in the world of investments, many continue fear the flood gate of claims before the courts on these lines. To begin with, cryptocurrencies are centred around computer networks and algorithms. There remains a great degree of ambiguity regarding its nature and owners. These queries have resulted in numerous discussions surrounding tax policies and the malicious activities stemming from such money. Regulation of cryptocurrencies is faced with challenges such as jurisdiction, possession, the purpose of the income acquired, etc. Accordingly, this paper evaluates India's cryptocurrency taxation regime through a comparative doctrinal lens, using Singapore's activity-based model as a benchmark to assess equity, certainty and administrative coherence. The article begins with a fundamental understanding of taxation, virtual digital assets and blockchains. This is followed by a brief insight into cryptocurrencies and a global perspective surrounding its definitions as well as their recognition. The write-up then presents a case study involving the taxation policies of Singapore and India in this regard. This analysis is based on the four Canons of Taxation propounded by Adam Smith. It concludes with legally implementable recommendations aimed at improving doctrinal clarity and administrative efficiency in the taxation of virtual digital assets.

Key Words: Crypto currency, taxation, blockchain

INTRODUCTION

The term tax refers to a rate or a sum of money assessed on the person or his/her/their property by the government to fulfil public needs(Aiyer, 2020). India's Apex Court has held that tax is a compulsory exaction of money by a public authority and is not merely a payment for services rendered. The act or the process of doing so is called taxation(Commissioner H.R.E. v Sri Lakshmanindra Thirtha Swamiar of Sri Shirur Mutt, 1954).This is also perceived

as a burden which is primarily borne by the State but transferred to the citizen(Commissioner H.R.E. v Sri Lakshmanindra Thirtha Swamiar of Sri Shirur Mutt, 1954)

Article 366(28) of the Constitution of India states that taxation includes the "imposition of any tax, or impost, whether general or local or special, and tax shall be construed accordingly."The obligations associated with such amounts stem from existing debts or the anticipation of similar scenarios.[1] Taxation is aimed at four purposes(Dr. Girish Ahuja):

1. Raise revenue for the government

2. Redistribute income and wealth from the rich to the poor people

3. Protect domestic industries from foreign competition

4. Promote social welfare.

There are three essential elements to taxes(Dr. Girish Ahuja). Firstly, the sum of money which is mandatorily payable must be ascertained. Secondly, the imposition of such payments must be legal. Thirdly, there must be clarity about the share of money that each party in question must bear. To this effect, one could assess a nation's taxation system based on Adam Smith's Canons of taxation.

There are four canons of taxation as laid down by Adam Smith in his book, 'The Wealth of Nations'. They are:

1. Canon of Equality: This refers to the principles of social justice or the ability to pay taxes. Taxes imposed must be proportionate to the income of the individual.
2. Canon of Certainty: This implies that there must not be any arbitrariness in the taxation system. This will build a trust between the taxpayer and the tax authorities.
3. Canon of Convenience: Convenience herein is regarding the payment mechanism. A complicated method to pay taxes would certainly deter people from doing so. Hence, the means to such payments must be easily comprehensible.
4. Canon of Economy: A good tax system is that where there are minimal administrative costs involved is the tax collection process.[2] Governments must strive to achieve this goal.

Interestingly, the OECD's Practice Note addresses these principles and has aligned the taxpayers' rights accordingly(Taxpayers' Rights and Obligations – Practice Note). For instance, the Charter explains that individuals have the Right to Certainty as well as the Right to Pay no more than the correct amount of tax. But developments in the business and trading arenas have paved the way for an array of complications in this respect. Uncertainty ranks high in the list of complexities herein. This facet has only enhanced with the onset of cryptocurrencies and the like.

REVIEW OF LITERATURE

In recent times, cryptocurrencies have become more than mere instruments with a certain perceivable value. They can also facilitate exchange and act as investable security(Gary Marchant, 2020). In 2020, the total number of crypto users across the world was recorded at 100 million(Thiemann). But there are several concerns surrounding their existence. To begin with, they are decentralised and have a limited supply chain(Bagis, 2022). Safety is yet another concern(Bagis, 2022). Researchers have stated that crypto markets have become a space for criminal activities ranging from bankruptcy, frauds and more(Katherine Baer, 2023).

RESEARCH OBJECTIVE

There are five main objectives behind this research. They are to:

1. To examine the doctrinal coherence of India's cryptocurrency taxation framework under the Income-tax Act, 1961.
2. To assess the compliance of Sections 115BBH and 194S with the principles of equity and certainty in taxation.
3. To comprehensively analyse India's approach with Singapore's activity-based taxation of digital tokens
4. To evaluate the scope for legally implementable reforms in cryptocurrency taxation without undermining regulatory oversight.
5. Make India more cryptocurrency-friendly

RESEARCH QUESTION

RQ1: Whether India's cryptocurrency taxation regime under Sections 115BBH and 194S of the Income Tax Act, 1961 complies with the principles of equity and certainty in taxation, when assessed against Singapore's activity-based taxation framework?

RESEARCH METHODOLOGY

The study herein is primarily a qualitative study, whilst exploring the correlation between cryptocurrency taxation mechanisms and economic progress. The analyses are based on a comparative evaluation of the policies of two common law jurisdictions situated in Asia. The criteria for the selection of these two nations include existing bilateral trade ties and the shared goals of progress in the space of digital finance.

The information used is based on primary and secondary sources of data. These included data available on government-approved platforms such as the Monetary Authority of Singapore, the Guidelines published by Inland Revenue Authority of Singapore and the Comprehensive Economic Cooperation Agreement between The Republic of India and the Republic of Singapore. It also analysed the Indian Supreme Court's position regarding the ambit of cryptocurrencies and their taxation. Further, the research involved the inputs provided in other academic publications related to virtual digital assets, digital finance, and

cryptocurrencies. It emphasises on the relevant Indian statutes such as the Income Tax Act of 1961 and the circular published by the Central Board of Direct Taxes (Circular No. 13/2022) regarding taxes imposed on virtual digital assets.

THEMATIC ANALYSIS

The research addresses common concerns such as the reliability of cryptocurrency and virtual digital assets. It acknowledges that 'new money' are based on computerised codes which are often incomprehensible by many investors. Further, it highlights that these forms of tender may be not legal recognised in many jurisdictions. Then again, they cannot be disregarded as illegal or valueless. To this effect, there is much debate about whether regulations in space of cryptocurrencies would only enhance the existing restrictions.

FINDINGS

India's cryptocurrency taxation regime reflects a revenue-centric design which, while legally enforceable, generates significant concerns relating to equity, compliance burden, and doctrinal consistency. The lack of definitional clarity—whether crypto constitutes capital asset, business income, or speculative income—creates doctrinal inconsistency. Scholars have observed that India's crypto taxation represents a case of revenue priority overwhelming regulatory coherence.Equity is compromised when compliance becomes a deterrent rather than a facilitator of lawful participation. The result is a paradox: while India seeks to tax virtual-asset income aggressively, its procedural design erodes the very tax base it aims to secure.

DISCUSSION

Different authorities across the world perceive 'Virtual assets' in varied ways. India's Income Tax Act of 1961 considers them to be those which can be digitally traded or transferred based on their value(Income Tax Act, 1961, s.115BBH). The International Monetary Fund (IMF), on the other hand, states that they are digital representations of value, issued by private developers and denominated in their own unit of account (International Monetary Fund). This view has been upheld by the Financial Action Task Force (FATF), but their functions include being a medium of exchange, and/or a unit of account, and/or a store of value(Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations, 2021). Some bodies also say these assets cannot be used as legal tender in any jurisdiction.

The common thread stringing the varied perceptions of virtual assets is cryptography and Distributed Ledger Technology (DLT). While cryptography is akin to computer programming, DLT records and shares data across multiple data stores (aka ledgers)(Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations, 2021).These records are maintained & controlled by the distribution of computer networks (nodes). Blockchains are an example in this regard. It was also used by an anonymous party to develop Bitcoin, a type of cryptocurrency.

Cryptocurrencies have received mixed responses across the globe. On the one hand, they are perceived as 'new money' and claims to entail many benefits. But on the other hand, their legitimacy continues to be debated. It is a subset of virtual assets. Yet their definition varies from nation to nation. In the United States of America (USA), for instance, the Internal Revenue Service (IRS) defines it as "atype of virtual currency that uses cryptography to secure transactions that are digitally recorded on a distributed ledger, such as a blockchain." Australia's Reserve Bank states that Cryptocurrencies are essentially digital currencies which people can use to pay each other, but they do not have any legislated or intrinsic value.

The European Central Bank provides a more futuristic definition. It describes cryptocurrencies as unregulated digital money, which is issued and usually controlled by their developers(Virtual Currency Schemes, 2012). They added that it is used as well as accepted among the members of a specific virtual community (Virtual Currency Schemes, 2012). Further, it explains that this perception is likely to be altered over a period, subject to the changes in the fundamental characteristics of the currency (Virtual Currency Schemes, 2012). India has not explicitly defined cryptocurrencies but has provided for the taxation of virtual digital assets. This has been mentioned in Section 115BBH and Section 194s of the Income Tax Act of 1961.

The ambiguity surrounding the nature of such tender has raised many concerns. The infringement of taxpayers' rights is among the primary issues. Its decentralised feature and absence of jurisdictional powers could lead to problems beyond the financial space. Yet, many countries have begun encouraging their residents to resort of this form of currency.

In May 2021, there were about 9,000 different cryptocurrencies with a market capitalisation of almost 2 trillion EUR. This was driven mainly by Bitcoin. During the same period, the market capitalisation of Bitcoin (about EUR 850 billion) ranked as the sixth largest. This was said to be higher than Facebook Inc. and lower than Alphabet Inc(Thiemann). Some jurisdictions have adopted a progressive taxation policy while some others have fixed tax brackets based on the period of holding or other criteria in relation to these investments.

But the concerns related to these investments appear to have a common thread. The absence of intermediaries is one such aspect. Many fear that these transactions could infringe their Right to Privacy owing to the lack of clarity about the parties managing these systems. There are, additionally, no clear approaches to make an appeal or raise grievances herein. This paves the way for malicious activities via the dark web. It would therefore be beneficial to the assess their strategies vis-à-vis India's existing taxation policy in this regard.

Case study: Cryptocurrency taxation in Singapore and India

Tax rates surrounding cryptocurrencies are subject various factors worldwide. One such aspect is the purpose behind their use. This determines the appropriate head under which income from cryptocurrencies can be included. The rates vary from Nil to as high as 55%. The systems in relation to this facet are more complex in some jurisdictions. For instance, the USA imposes different tax rates upon cryptocurrencies across the country. Dubai, on the other hand, does not tax those who engage in cryptocurrency transactions.

Then again, effective tax policies could prove favourable in the space of new money and its impact on the economy. Singapore is one such example. Their strategies are relevant in this context owing to their pivotal role in India's trade and commerce. This has been further enhanced through the India–Singapore Comprehensive Economic Cooperation Agreement (CECA) of 2005(Comprehensive Economic Cooperation Agreement between The Republic of India and the Republic of Singapore).The Agreement herein has been reviewed by these nations over the years. The most recent revision was made in 2022 to explore digital trade and green technology.

It is noteworthy that bilateral merchandise and services trade reached roughly USD 35–36 billion in FY 2023–24. Singapore has also been a leading source of Foreign Direct Investment (FDI) into India. The country saw large equity inflows channelled via Singapore in FY 2023–2024(Comprehensive Economic Cooperation Agreement between The Republic of India and the Republic of Singapore). In recent times, India and Singapore have extended their cooperation's in areas such as fintech and payments connectivity (notably UPI-Pay Now interoperability), start-up collaboration, and clean-technology partnerships.

It must be noted that Singaporeis a highly open, service-oriented, advanced economy with a long record of policy stability, outward orientation and institutional capacity for financial and technological innovation. The Monetary Authority of Singapore (MAS) acts as both central bank and integrated financial regulator and has an explicit fintech-enabling mandate.[3] Singapore's headline corporate tax rate remains competitive at 17%, supported by targeted incentives and a broad treaty network that facilitates cross-border investment.

India, on the other hand, appears hesitant on this front. In contrast to Singapore, its average monthly-spends on cryptocurrency per capita is $60(Study shows 1 in 2 financially savvy Singaporeans own crypto, bullish on its future, n.d.). It can hence be deduced that India is not as crypto-ready as its Asian trading partner. In 2021, the United Nations Trade and Development (UNCTAD) stated that only seven per cent of Indians invest in cryptocurrencies, unlike in Singapore, 9% of the population owns cryptocurrencies. Additionally, in 2024, a study reported that 57% of Singapore's financially sound individuals own cryptocurrencies(Study shows 1 in 2 financially savvy Singaporeans own crypto, bullish on its future, n.d.).

Scope of equity

Equity, in the tax arena, goes beyond arithmetic and deductions. In tax jurisprudence, procedural equity implies that taxpayers are treated uniformly under clear and predictable laws. It further explains that compliance does not impose an undue burden relative to the taxpayer's capacity. Singapore's system exemplifies this principle through its streamlined administrative mechanisms, transparent guidance, and proportionate enforcement.

The Inland Revenue Authority of Singapore (IRAS) has published detailed e-Tax Guides clarifying the income tax treatment of digital tokens, categorising them into payment, utility,

and security tokens(Income Tax Treatment of Digital Tokens 3 (e-Tax Guide), 2020).[3] This classification determines whether a transaction is taxable, with income derived from trading or business activity being subject to ordinary income tax, while mere capital appreciation remains outside the tax net(Income Tax Treatment of Digital Tokens 3 (e-Tax Guide), 2020). The approach, therefore, aligns with Singapore's overarching principle of technological neutrality, i.e. taxation based on the nature of the activity(Income Tax Treatment of Digital Tokens 3 (e-Tax Guide), 2020). For example, if a cryptocurrency (say Bitcoin) is used to buy and sell goods on an e-commerce platform, the income earned therein would fall under the head 'Income from Business'. Whereas when such currencies are considered as Capital Gains (like the conventional definition of the term), then they are not taxed as per the country's tax policies.

India's system, in contrast, is more rigid. It also entails much compliance. The Finance Act of 2022(Finance Act, 2022)inserted Section 115BBH into the Income-tax Act, 1961. This provision imposes a flat 30 percent tax on income from the transfer of Virtual Digital Assets (VDAs). The section explicitly prohibits any deduction other than the cost of acquisition and bars the set-off or carry-forward of losses(Section 115BBH). Further, Section 194S mandates a one-percent tax deducted at source (TDS) on every VDA transfer, regardless of profitability. While the new law was aimed at curbing money-laundering and speculative trading, it has created a compliance regime which has further burdened small investors and start-ups. The Central Board of Direct Taxes (CBDT) subsequently issued Circular No. 13/2022 to clarify certain operational aspects of Section 194S, but ambiguities persist—particularly regarding valuation, airdrops, and peer-to-peer transfers(Circular No. 13/2022 - Guidelines for Removal of Difficulties under Section 194S(6) of the Income-tax Act, 1961, 2022).[4]

Convenience and ease of transactions

Singapore is perceived to be a crypto-friendly country. In 2024, it was also the highest-ranking crypto-ready city in the Asian market, while globally, Singapore stood fifth (after New York, London, Los Angeles, and Sydney)(Most Crypto-ready Cities of 2024, 2024). A study also showed that the average monthly spending on cryptocurrency per capita is $2,681 in Singapore. This is equivalent (approximately) to the average monthly rent in the country.

Convenience in taxation is key to ensuring equity among taxpayers. In Singapore, compliance for crypto investors is rather straightforward. The IRAS integrates crypto-related income reporting into existing tax forms, eliminating the need for specialised schedules(Filing Individual Income Tax Returns, 2024). As Singapore does not impose capital-gains tax, casual investors, i.e. people who buy and hold crypto assets for personal purposes, need not report such holdings(Filing Individual Income Tax Returns, 2025). Income arising from professional trading, however, is taxed at the prevailing corporate or personal income-tax rates, which are progressive for individuals. This is capped at 17 percent for

corporations(Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard, 2022). The simplicity of the country's tax system, therefore, fosters voluntary compliance and administrative economy.

The IRAS guidance also aligns with the OECD's Crypto-Asset Reporting Framework (CARF), facilitating standardised disclosure and cross-border cooperation without imposing excessive domestic compliance obligations(MAS Notice PSN02: Prevention of MoneyLaundering and Countering the Financing of Terrorism – Digital Payment Token Service Providers).Further, Singapore's AML (Anti-Money Laundering) and CFT (Countering the Financing of Terrorism) frameworks have proven to be efficient to identify and prevent the misuse of financial systems for illicit or terrorist financing. Under the MAS Notice PSN02 (Prevention of Money Laundering and Countering the Financing of Terrorism), crypto service providers are required to conduct customer due diligence, monitor transactions, and report suspicious activities(MAS Notice PSN02: Prevention of MoneyLaundering and Countering the Financing of Terrorism – Digital Payment Token Service Providers). This approach ensures transparency and market integrity without stifling innovation through outright bans.

India's crypto-tax framework, on the other hand, scores poorly on convenience. Investors must track each transaction for Tax Deducted at Source (TDS) compliance, file additional disclosures under Schedule VDA(Notification No. 04/2023: Filing Requirements for Schedule VDA). Hence, they must also bear the cost of extensive record-keeping. The multiplicity of reporting obligations spikes costs for taxpayers and authorities. Further, the statutory scheme lacks an authority equivalent to Singapore's Monetary Authority of Singapore (MAS). This results in fragmented coordination between fiscal and financial regulators and deepens uncertainty. Additionally, the flat-rate taxation policy coupled with non-deductibility of losses distorts investment behaviour. This will discourage legitimate market activity while illicit users continue to exploit the markets.

From a doctrinal standpoint, equity is violated when unequal taxpayers are treated identically under a rigid statutory scheme. Singapore's differentiated approach—taxing only business-like crypto activity—upholds the principle of proportionality, whereas India's uniform 30 percent levy disregards context and capacity. The denial of loss offsets further contradicts the canon of equity by taxing gross rather than net gains. Policy-wise, Singapore demonstrates that convenience and efficiency can coexist with revenue integrity. Its model minimises administrative friction while maintaining sufficient oversight through CARF participation and MAS supervision. India's framework, while motivated by legitimate enforcement concerns, would achieve greater equity by adopting graded taxation and clearer classification guidelines. A balanced system must integrate doctrinal coherence (consistency with general tax principles) and policy pragmatism (ease of compliance and administrative feasibility).

Contesting certainty, convenience, and efficiency

Certainty surrounding such income stems from the perceptions held by those involved in the crypto ecosystem. The high scores and ranking in terms of Singapore's crypto- readiness also

reflect the effectiveness of its regulatory framework and the public's faith in digital assets. Also, Singapore's laws clearly state the nature and treatment of such funds.

India's broad and vague provision on these lines, on the other hand, defeats the purpose. The country's technological advancements are laudable, but it ceased to ensure active investments related to virtual assets. This is inferred from the number of people who can access platforms and possess the knowledge to engage in such trade. It thus questions the taxpayer's faith in the policy at hand. Such scenarios also discourage digital investments in the future.

Singapore's current digital assets taxation system does not impose any capital gains or sales tax on businesses or individuals for the purchase and profit made by the value appreciation of cryptocurrencies. Instead, it entails an income tax rate of 17%, which includes business or professional income from trading of bitcoin, which will be taxed. On the other hand, GST is not applied to these transactions if the payment for the product and services is made with cryptocurrencies (Bitcoin and Ether).

Interestingly, the IRAS's Income Tax Treatment of Digital Tokens guide, updated periodically, provides examples of taxable and non-taxable scenarios, ensuring taxpayers understand their obligations. The MAS complements this with clear licensing requirements for digital-payment-token service providers under the Payment Services Act 2019, thereby harmonising tax and regulatory treatment.[15]These measures collectively strengthen public confidence and encourage participation in the crypto economy. Studies indicate that more than 40 percent of Singapore's financially literate population holds cryptocurrencies, reflecting both trust and perceived fairness in the system.[5]

CONCLUSIONS

One cannot chide away from new money. This stance has upheld in the case of *IAMAI v RBI.* (IAMAI v RBI, 2020). The Indian Supreme Court herein legalised cryptocurrency exchanges and explained that the definition of money as well as currency changes with time. In a recent judgment of the High Court of Madras, the Court granted cryptocurrencies the status of 'property'. The pronouncement also elaborated that these currencies are capable of being owned, enjoyed and held in trust(Rhutikumari v. Zanmai Labs Pvt. Ltd. & Ors, 2025).

While India's cryptocurrency taxation framework under Sections 115BBH and 194S is legally enforceable, it raises substantial concerns relating to equity, certainty, and proportionality in taxation. In contrast, Singapore's activity-based taxation model illustrates that regulatory oversight and administrative efficiency can coexist with doctrinal coherence, without necessitating uniform or punitive tax treatment."

The current era demonstrates how algorithms determine interpersonal communications and the future of enterprises. To this effect, taxation and regulation of new tech-driven currencies do not curb their usage. On the contrary, they ensurebalance for to facilitate the fair

circulation of money. This will instil greater acceptance among the public and authorities. The result of such strategies is steady and meaningful economic and social growth.

SUGGESTIONS

Financial prosperity of a country demands adherence to Adam Smith's Canons of Taxation. It is only when the principles of equity, convenience, certainty, and economy are upheld that a nation witnesses a favourable circulation of currency. The need for mechanisms to address these facets are more relevant today owing to the dynamic nature of businesses. Further, cross-border transactions are no longer a matter of good fortune; it is quintessential of enterprises today.

India may consider strengthening its internal regulatory framework governing cryptocurrency transactions through coordinated statutory and regulatory measures. One significant initiative in this regard could be the establishment of a committee that is akin to the Monetary Authority of Singapore,[6] a quasi-governmental body. This organisation can provide relevant insights related to the developments related to digital transactions and the latest trends.

OTHER RECOMMENDATIONS INCLUDE THE FOLLOWING:

1. India's financial laws must pave the way for including newer forms of money and transactions. The language of such laws must not deter taxpayers from fulfilling their duties. On the contrary, they must motivate them to comply with the statutes in letter and spirit. This will ensure steady circulation of funds in the economy.

2. Lawmakers must involve the public in matters concerning drafts associated with tax and finance laws. This not only reaffirms the spirit of democracy but also paves the way for a participatory approach in policymaking. It will also enable the leaders of a nation to devise mechanisms catering to the needs of the people. This will ensure convenience and certainty in the tax regime.

3. The authorities must educate all residents, including those residing in rural India, about digital currencies and their role in the present banking sector. They must strive towards strengthening the infrastructure for such purposes and upskill personnel to this effect. Further, they should equip them with tools to protect themselves from the misuse of such transactions. Training programmes and initiatives in the local dialect can prove beneficial in these cases.

4. India's tax laws must clearly define cryptocurrencies and not include them within the large umbrella called Virtual Digital Assets (VDA). In doing so, the authorities will encourage more investments or transactions using new currencies. It will also rid all fears associated with the same. This will enhance online business activities and help assess the true scope of this form of financial tender. This will enable the relevant authorities to determine the appropriate heads for income related to cryptocurrencies.

5. Uniform conversion systems can help promote trade and exchange of such money. This will ensure a greater degree of accountability and tackle nefarious activities across the internet. The existing CECA between Singapore and India can include provisions to do so. This could be assessed over a reasonable period and modified according to the data so acquired in this regard.

LIMITATIONS

One of the greatest limitations of this study is the absence of adequate precedents. Cryptocurrencies and other virtual digital assets are relatively new entrants to the world economy. More importantly, India's demography is unique. Financial management in the country adorns a new flavour owing to several cultural and societal reasons. The preferences for in this regard are subject to the levels of risk one is willing to undertake too. This factor varies across different strata. Hence, it is tedious to draw parallels regarding the strategies on these lines owing to the varied scope of such money across jurisdictions.

Further, cryptocurrencies are not bound by any centralised issuance system. They are also not monitored by central administrators or financial intermediaries. This sense of anonymity could prove to be fearsome. These characteristics complicate the application of the canon of certainty in taxation, particularly in identifying taxable events and accountable parties. Lastly, the lack of standardised taxation systems and values assigned to cryptocurrencies across jurisdictions paves the way for tax evasion, money laundering, and other illicit activities. This adds to the problems related to double taxation as well. Each of these aspects adds to the burden of determining their impact in the large economic scheme.

SCOPE FOR FUTURE RESEARCH

Technological developments and increased digitisation of lifestyles will certainly create more avenues for such research. Given the dynamic nature of the current business environment, digital finance and various players in the space are likely to play a pivotal role. An in-depth analysis about how the courts in both economies perceive such currencies and relevant transactions can provide better inputs for effective policies. Further, it would be beneficial to see how traders and commercial markets grow through the implementation of favourable cryptocurrency usage.

REFERENCES

- Bilal Bagis, *Digital Currencies and Monetary Policy in the New Era,* Insight Turkey, Vol. 14, 2022.
- Chainanalysis - Cryptocurrencies: An Empirical View from a Tax Perspective by Andreas Thiemann, 2021.
- Central Board of Direct Taxes, Circular No. 13/2022.
- Commissioner H.R.E. v Sri Lakshmanindra Thirtha Swamiar of Sri Shirur Mutt, Supreme Court, 1954.

- Comprehensive Economic Cooperation Agreement between The Republic of India and the Republic of Singapore, https://www.commerce.gov.in/international-trade/trade-agreements/comprehensive-economiccooperation-agreement-between-the-republic-of-india-and-the-republic-of-singapore/, accessed on November 5, 2025.
- Cryptocurrency Tax in Singapore, https://relinconsultants.com/cryptocurrency-tax-singapore/#singapore-tax-treatment, accessed on December 25, 2025.
- Digital Payment Tokens, https://www.iras.gov.sg/taxes/goods-services-tax-(gst)/specific-business-sectors/digital-payment-tokens, accessed on April 26, 2025.
- Dr. Girish Ahuja, Dr. Ravi Gupata, CA. Kriti Chawla, Principles of Taxation, 2nd Edition, Commercial Law Publishers (India) Pvt Ltd.
- Finance Act, 2022, No. 6, S 3, India Code (LexisNexis through 2025).
- Gary Marchant, Jalaj Jain, et al, *International Governance of Cryptoassets*, The International Lawyer, Vol. 53, 2020.
- Guidelines for Removal of Difficulties under Section 194S(6) of the Income-tax Act, 1961, June 22, 2022.
- *IAMAI v RBI*, 2020 SCC online SC 275.
- Income Tax Act, 1961, s.115BBH
- Inland Revenue Authority of Singapore, Filing Individual Income Tax Returns, 2024.
- Inland Revenue Auth. of Sing., Income Tax Treatment of Digital Tokens 3 (Oct. 9, 2020) (e-Tax Guide).
- Katherine Baer, Ruud De Mooij, et al, *Taxing cryptocurrencies*, Oxford Review of Economic Policy, Vol. 39, 2023.
- Monetary Authority of Singapore,https://www.mas.gov.sg/, accessed on April 26, 2025.
- Monetary Authority of Singapore, *MAS Notice PSN02: Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Payment Token Service Providers*, https://www.mas.gov.sg/regulation/notices/psn02, accessed on Nov. 3, 2025.
- Most Crypto-ready Cities 2024,https://coinwirez.com/most-crypto-ready-cities-2024/, accessed on April 26, 2025.
- Organisation for Economic Co-operation & Development, *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*, 2022.
- P Ramanathan Aiyar, The Law Lexicon, Fifth Edition, 2020.
- *Rhutikumari v. Zanmai Labs Pvt. Ltd. & Ors*, 2025:MHC:2437
- Section 115BBH, Income Tax Act of 1961.
- Study shows 1 in 2 financially savvy Singaporeans own crypto, bullish on its future, https://sbr.com.sg/financialservices/news/study-shows-1-in-2-financially-savvy-singaporeans-own-crypto-bullish-its-future, accessed on April 26, 2025.
- Taxpayers' Rights and Obligations – Practice Note, https://www.oecd.org/content/dam/oecd/en/topics/policyissues/tax-administration/taxpayers-rights-and-obligations-practice-note.pdf, accessed on October 23, 2025.
- Vincent Ooi, The Taxation of Cryptocurrency Gains, Bulletin for International Taxation, 2021.

- Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations, International Monetary Fund, 2021.
- Virtual Currencies and Beyond: Initial Considerations, International Monetary Fund, 2016.
- Virtual Currency Schemes, European Central Bank, 2012.

DIGITAL ASSETS AND THE LAW: AN INDIAN PERSPECTIVE WITH COMPARATIVE INSIGHTS FROM THE US AND UAE

Tassaduq Hussain
Fourth-Year, B.A.LL. B (Hons.) Student,
School of Law, University of Kashmir, Srinagar, J&K

Abstract

Digital assets have rapidly emerged as a defining feature of the global financial ecosystem. Cryptocurrencies, stablecoins, non-fungible tokens (NFTs), and Central Bank Digital Currencies (CBDCs), all rooted in blockchain technology, are reshaping our understanding of value, ownership, and financial systems. In India, while adoption has surged, the regulatory and legal framework remains fragmented, reactive, and ambiguous. Against this backdrop, the research highlights India's lack of a coherent, innovation-positive legal framework that strikes a balance between financial stability and technological growth. Employing a doctrinal and comparative methodology, the study examines statutes, case law, regulatory notifications, and scholarly commentary. It reviews existing literature to highlight the research gap and situates India's regulatory efforts within an international context. The analysis reveals that while India focuses primarily on taxation and anti-money laundering measures, the US prioritises investor protection through enforcement, and the UAE fosters innovation through structured classifications and licensing. The paper concludes that India must adopt a hybrid model that combines clarity in classification, coordinated regulation, investor safeguards, and regulatory sandboxing. Such a framework will not only mitigate risks but also enable India to emerge as a leading jurisdiction in digital asset regulation.

Key Words: ***Digital Assets, Virtual Digital Assets (VDAs), Blockchain Technology, Cryptocurrency Regulation, Central Bank Digital Currencies (CBDCs), Comparative Law, Regulation, Investor Protection, Taxation***

INTRODUCTION

*"Regulatory ambiguity is the greatest threat to the potential of digital assets. Innovation thrives on clarity." – Chris Dixon, General Partner, Andreessen Horowitz.*Digital assets have rapidly emerged as a defining feature of the contemporary financial landscape. Their disruptive potential has challenged traditional regulatory frameworks across jurisdictions. In India, the regulatory trajectory has been cautious and fragmented, characterised by temporary restrictions, taxation measures, and selective application of existing statutes. This uncertainty has led to both investor anxiety and policy debate. In contrast, other jurisdictions have adopted more structured approaches, such as the US, with its evolving enforcement and legislative model, and the UAE, with its innovation-driven framework.

This paper examines these comparative approaches to highlight lessons for India. By situating India's regulatory dilemma alongside the USand UAE, it explores how a hybrid model can balance innovation, systemic stability, and investor protection.

RESEARCH PROBLEM

The rapid proliferation of digital assets has created a disruptive financial ecosystem that challenges traditional legal and regulatory paradigms. In India, while tax recognition and Anti-Money Laundering (AML) inclusion have been introduced, there is no comprehensive legal framework to govern digital assets. This results in ambiguity regarding classification, investor protection, and innovation. A key concern is the absence of an "innovation-friendly framework," which in practical terms would mean a regime that provides legal clarity, proportionate compliance obligations, access to regulatory sandboxes, and support for new business models without excessive restrictions. Such a framework would encourage technological development while ensuring consumer safeguards.

By contrast, India's current approach reflects a "risk-averse framework," characterised by blanket prohibitions (such as the erstwhile RBI banking ban), heavy taxation, and reactive compliance measures that discourage entrepreneurship and investment in the sector. These contrasting approaches can be measured by whether regulation provides clarity, promotes experimentation, and fosters responsible growth, or whether it imposes deterrent costs and uncertainty that stifle innovation.

In contrast, other jurisdictions have adopted more structured approaches that highlight India's regulatory gap. The US has relied on enforcement-led oversight and, more recently, moved towards asset-specific legislation such as the *GENIUS Act* for stablecoins, which balances investor protection with innovation. The UAE, by comparison, has established an innovation-oriented framework through clear asset classification and licensing, attracting global digital asset businesses. These examples illustrate that India's problem is not one of global impossibility, but of a regulatory choice.

Furthermore, the regulatory challenge in this field is inherently temporal. Digital asset technologies and markets evolve at a pace that outstrips conventional law-making. Any framework that is too rigid or delayed risks becoming obsolete by the time it is implemented. Thus, the research problem is not only the absence of a coherent and balanced framework in India, but also the urgent need for a regulatory model that can adapt dynamically to the fast-changing nature of digital assets.

RESEARCH OBJECTIVES

1. To trace the evolution and conceptual foundations of digital assets globally and in India.
2. To critically analyse the legal and regulatory framework of digital assets in India.
3. To compare India's regulatory stance with the approaches adopted by the US and UAE.
4. To identify regulatory gaps in India and suggest reforms that balance innovation with investor protection.

RESEARCH QUESTIONS

1. How are digital assets defined and classified in India compared to the US and UAE?
2. What are the primary legal and regulatory challenges India faces in regulating digital assets?
3. What lessons can India learn from the USand UAE regulatory models?
4. How can India develop a coherent, innovation-friendly, and risk-based framework for digital assets?

RESEARCH METHODOLOGY

This paper adopts a doctrinal and comparative legal research methodology. The doctrinal approach involves a detailed study of statutory provisions such as the *Income-tax Act, 1961*, the *Prevention of Money Laundering Act, 2002*, and regulatory measures issued by the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI). Judicial precedents, most notably *Internet and Mobile Association of India v. Reserve Bank of India*, have been examined directly from primary sources. In the US, primary legal materials such as regulatory enforcement actions and statutory developments were accessed in English, supplemented by academic commentary. With respect to the UAE, official English translations of statutory texts and regulatory frameworks were consulted where available; however, due to the linguistic barrier posed by Arabic primary sources, the analysis has been supplemented by secondary academic and policy literature. Secondary sources across all jurisdictions—including scholarly articles, reports from international organisations (IMF, FATF, WEF), and policy papers—have been employed to enrich and contextualise the doctrinal analysis.

SCOPE AND LIMITATIONS

The scope of this paper is confined to the legal and regulatory dimensions of digital assets in India, with comparative references to the US and UAE. It does not delve into the technological coding or economic forecasting aspects of digital assets. The study is limited to statutory, regulatory, and judicial frameworks up to August 2025.

LITERATURE REVIEW

Scholarly work on digital assets has primarily revolved around their disruptive potential and regulatory challenges. *Zetzsche, Buckley, and Arner* highlight how the US has developed a fragmented, enforcement-led regulatory model, raising concerns about legal uncertainty and investor protection.[1]The International Monetary Fund has underscored the risks of regulatory arbitrage and called for global coordination to ensure financial stability in the digital asset space.[2] Similarly, the Financial Action Task Force has provided detailed guidance on applying anti-money laundering (AML) and combating the financing of terrorism (CFT) standards to

[1]Dirk A. Zetzsche, Ross P. Buckley & Douglas W. Arner, *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation, 23 Fordham J. Corp. & Fin. L. 31, 45-52 (2017).*

[2] Int'l Monetary Fund, *Global Financial Stability Report: Cryptoassets as the Future of Money?* (Oct. 2021), https://www.imf.org/en/Publications/GFSR/Issues/2021/10/12/global-financial-stability-report-october-2021.(last visited May 15, 2025).

virtual assets and service providers.[3] In contrast, policy reports examining the United Arab Emirates—such as the Dubai Virtual Assets Regulatory Authority framework—illustrate a proactive and innovation-friendly regulatory approach, positioning the UAE as a model for emerging economies.[4]

While these contributions are valuable, two types of research gaps are evident. First, in terms of substantive gaps, most Indian literature remains descriptive, focusing either on taxation, AML inclusion, or the Reserve Bank of India's prohibition, without offering a systematic comparative analysis. Comparative studies, when they exist, typically examine India in relation to a single jurisdiction (often the US or the EU). The UAE's innovation-oriented model, which contrasts sharply with India's cautious stance, has received little comparative attention alongside US enforcement practices.

Second, and more importantly, there are methodological gaps. Much of the existing scholarship employs a black-letter or doctrinal approach in isolation, describing statutory developments without embedding them in a broader comparative or policy framework. Few works attempt a structured cross-jurisdictional comparison that brings together India, the US, and the UAE in a single analytical framework. Even fewer integrate doctrinal analysis with forward-looking, innovation-focused evaluation of regulatory sandboxes, investor safeguards, or adaptive mechanisms. This lack of methodological diversity limits the ability of existing studies to propose context-specific yet globally informed reforms.

This paper, therefore, addresses both the substantive and methodological gaps. It contributes uniquely by situating India's regulatory dilemma within a three-jurisdiction comparative framework, drawing on the US's enforcement-driven approach and the UAE's innovation-driven model. By combining doctrinal analysis of statutory provisions, regulatory notifications, and judicial precedents with comparative insights from multiple jurisdictions, the study advances a normative recommendation for India: the design of a balanced and innovation-positive framework informed by global best practices.

HISTORICAL BACKGROUND

A. Conceptual Foundations and Early Innovations (Late 20th Century):

The conceptual foundations of digital assets started gaining ground in the late 20th century with the inception of electronic cash systems. In 1998, cryptographer *Nick Szabo* proposed *"Bit Gold,"*[5]a conceptual decentralised digital currency that would allow for secure, trustless transactions without intermediating authorities by having users solve cryptographic puzzles and using a proof-of-work (PoW) mechanism to validate submissions. Although "Bit Gold" was

[3] Fin. Action Task Force, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (June 2019), https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.(last visited May 15, 2025).
[4] Dubai Virtual Assets Regulatory Authority (VARA), *Regulatory Framework for Virtual Assets* (2022), https://www.vara.ae/en/regulations(last visited May 15, 2025).
[5]Nick Szabo, Bit Gold (Dec. 29, 2008), https://unenumerated.blogspot.com/2005/12/bit-gold.html.(last visited August 10, 2025).

never actualised as a system or method of digital currency, it recommended resolutions to significant issues related to double-spending and making value-verification claims. Szabo, therefore, established a foundational intellectual and technical basis that would later facilitate, organise, and inspire the proliferation of Bitcoin-style currencies and associated innovations. Szabo's anticipated decentralised digital scarcity foreshadows the justifications that characterise many blockchain-based assets today and exemplify the tension between digital and traditional cash systems, economies, and cultures.[6]

B. Emergence of Cryptocurrencies and Blockchain Technology (2009–2013):

Cryptocurrencies made their debut in 2009 with the launch of Bitcoin, created by an individual or group under the pseudonym *Satoshi Nakamoto*. Bitcoin is a cryptocurrency that operates on blockchain technology, i.e. a distributed ledger that enables peer-to-peer transactions without the need for intermediaries. By addressing the double-spending problem in digital currency and introducing a transparent and secure method for direct transactions between parties, Bitcoin paved the way for the emergence of numerous other cryptocurrencies. These alternative cryptocurrencies were designed either to improve upon Bitcoin's model or to define their own niche within the growing cryptocurrency market.[7]

C. Diversification and Technological Advancements (2014–2017):

In 2015, the digital asset ecosystem expanded in scope and shape with the launch of Ethereum, which offered developers a new way to create decentralised applications (dApps) and smart contracts (i.e., self-executing contracts with the terms of the agreement written directly into code). In addition, ICOs (Initial Coin Offering) during this timeframe emerged as a new method of raising capital for startups and blockchain projects, allowing founders to issue tokens in exchange for future project-related revenues. However, as projects began conducting ICOs, an increasing focus on funder protection began to emerge.[8]

D. Institutional Adoption and Regulatory Responses (2018-Present):

This phase was marked by heightened institutional interest, with global banks investigating blockchain applications and the development of cryptocurrency services.Regulators across the world began formulating frameworks to deal with the challenges posed by digital assets. As an example, the *US Securities and Exchange Commission* (SEC) applied existing securities laws to digital assets in light of the debates surrounding appropriate classifications and compliance as they transition to digital assets. At the same time, the *Financial Stability Oversight Council*

[6]Filippo Zatti & Rosa Giovanna Barresi eds., *Digital Assets and the Law: Fiat Money in the Era of Digital Currency* (Routledge 2023).

[7]Swift Inst., *Defining Digital Assets: Past, Present, Future* (2022), https://www.swift.com/swift-resource/251789/download (last visited May 15, 2025).

[8]Wulf A. Kaal, Digital Asset Market Evolution, 45 J. CORP. L. 47 (2019).

(FSOC) evaluated the risks associated with the financial stability posed by cryptocurrency and focused on the need for adequate regulatory oversight.[9]

E. Integration with Traditional Financial Systems and Emerging Trends (2020s):

During the 2020s, there have been attempts to integrate digital assets into the mainstream financial system. Central banks are working on CBDCs, which would, to some measure, offer the benefits of digital assets and the trust of fiat. The tokenisation of real-world assets, such as real estate and commodities, is also being explored, which could increase liquidity and accessibility in markets.[10] Regulatory approaches continue to evolve, with jurisdictions adopting diverse strategies to strike a balance between innovation, consumer protection, and financial stability.[11]

UNDERSTANDING DIGITAL ASSETS

Building upon the historical trajectory of digital innovations, a nuanced comprehension of 'digital assets' themselves is fundamental to navigating their complex legal and regulatory landscape. This section aims to establish a comprehensive conceptual framework by first examining global definitional perspectives from leading international bodies and then detailing the diverse categories of these assets, from cryptocurrencies to CBDCs. Finally, it will distil the specific Indian legal definition of digital assets, highlighting its scope and implications within the Indian context. This foundational understanding is crucial before exploring the regulatory responses they have elicited across various jurisdictions.

A. Global Perspective

As per the *Financial Action Task Force (FATF*), 'A digital asset is a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Digital assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.'[12]

The *International Monetary Fund (IMF)* posits that digital assets are digital representations of value made possible by advances in cryptography and distributed ledger technology. They may

[9]Cong. Research Serv., Digital Assets and SEC Regulation, CRS Report R46208 (2023), https://crsreports.congress.gov/product/pdf/R/R46208(last visited June 15, 2025).
[10]World Econ. F., Digital Assets Regulation: Insights from Jurisdictional Approaches (2023), https://www3.weforum.org/docs/WEF_Digital_Assets_Regulation_2024.pdf(last visited May 15, 2025).
[11].P. Morgan, The Evolution of Digital Assets (2023), https://www.jpmorgan.com/content/dam/jpm/cib/complex/content/securities-services/regulatory-solutions/evolution-of-digital-assets.pdf(last visited May 15, 2025).
[12]Fin. Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Oct. 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf(last visited May 15, 2025).

be used as a medium of exchange, unit of account, or store of value and may or may not have legal tender status.[13]

The *World Economic Forum (WEF)* defines digital assets as a new asset class based on blockchain infrastructure, encompassing cryptocurrencies, stablecoins, utility tokens, NFTs, and tokenised versions of traditional assets.[14]

B. Types of Digital Assets

1. Cryptocurrencies: These are decentralised digital currencies that operate independently of any central bank or government. They operate on blockchain technology to record and verify transactions through consensus mechanisms like PoWor Proof-of-Stake (PoS). Examples include Bitcoin and Ethereum.
2. Stablecoins: Stablecoins are digital tokens designed to maintain a stable value by being pegged to an underlying reserve asset, such as fiat currency or commodities. They are commonly used to facilitate trading and remittances within the crypto ecosystem without exposure to volatility. Examples include Tether and Paxos Gold.
3. Non-fungible tokens (NFTs): NFTs represent unique digital assets and are stored on a blockchain, making them indivisible and non-interchangeable. They are frequently used in digital art, gaming, intellectual property, and virtual identities. Examples include CryptoPunks and Bored Ape Yacht Club (BAYC).
4. Security tokens: Security tokens confer ownership rights or revenue shares in an enterprise or asset and are often governed by securities law, e.g. tZERO – a regulated trading platform offering tokenised equity.
5. Utility tokens: Theyprovide access to a service, feature, or network but do not imply ownership or investment returns, e.g. Basic Attention Token (BAT) – used for incentivising users and creators within the Brave browser ecosystem.
6. Central bank digital currencies (CBDCs): CBDCs are digital legal tenders issued and backed by a country's central bank, representing a digital form of fiat currency. They aim to offer the safety and stability of traditional money with the convenience of digital transactions. Examples include Digital Rupee (e₹), Digital Yuan (e-CNY) and Sand Dollar.

C. Indian Perspective

A legal definition of digital assets was introduced in India for the first time through the *Finance Act, 2022*, with the insertion of Section 2(47A) into the *Income Tax Act, 1961*. The term *"Virtual Digital Asset"* is defined as follows:

"Virtual Digital Asset" means—

[13]Int'l Monetary Fund, *The Ascent of Digital Money*, IMF Staff Discussion Note SDN/19/01 (July 2019), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2019/06/27/The-Ascent-of-Digital-Money-46966(last visited May 19, 2025).

[14]World Econ. F., *Digital Assets Regulation: Insights from Jurisdictional Approaches* (Jan. 2023), https://www3.weforum.org/docs/WEF_Digital_Assets_Regulation_2024.pdf(last visited May 15, 2025).

(a) any information, code, number or token (not being Indian currency or any foreign currency), generated through cryptographic means or otherwise, by whatever name called, providing a digital representation of value exchanged with or without consideration, with the promise or representation of having inherent value, or functions as a store of value or a unit of account, and includes its use in any financial transaction or investment, but not limited to investment schemes;

(b) a non-fungible token or any other token of similar nature, by whatever name called;

(c) any other digital asset, as the Central Government may, by notification in the Official Gazette, specify.[15]

This definition excludes government-issued currencies like the Digital Rupee and foreign fiat currencies, thereby solelyfocusing on privately issued digital assets like cryptocurrencies and NFTs.

LEGAL AND REGULATORY FRAMEWORK OF DIGITAL ASSETS IN INDIA

Having established a global and Indian definitional framework for digital assets, including their various types and the unique challenges they present, the focus now shifts to how these novel instruments are being addressed within India's legal and regulatory landscape. The diverse characteristics of these assets, from cryptocurrencies to NFTs and CBDCs, necessitate specific regulatory considerations. This section will critically analyse the current fragmented and multi-agency approach adopted by India, examining the implications of statutory recognitions, regulatory guidance, and judicial interventions.

At present, India lacks a cohesive legal framework for regulating digital assets. India's regulation of digital assets is occurring on a piecemeal and multi-agency basis, inclusive of tax authorities, the Reserve Bank of India (RBI), the Financial Intelligence Unit (FIU-IND) and the Enforcement Directorate (ED). Digital assets have been legally defined for tax purposes, but there is no statute or regulatory code that governs their creation, trading, and overall legal position.

A. Statutory Recognition: The Income Tax Act, 1961

The Finance Act, 2022, represented the first major impetus for official recognition of digital assets within India when it amended the Income Tax Act, 1961, and defined the term "Virtual Digital Assets." The definition under Section 2(47A) includes any information, code, number, or token generated through cryptographic means or otherwise, having a digital representation of value that can be transferred, stored or traded electronically, excluding Indian and foreign currencies. Now, under the Income Tax Act, 1961:

[15]Gov't of India, *Finance Act, 2022*, § 2(47A); Income Tax Dep't of India, https://incometaxindia.gov.in(last visited May 29, 2025).

1. Section 115BBH imposes a flat 30% tax on income generated from the transfer of VDAs.[16]
2. Section 194S introduces a 1% TDS (Tax Deducted at Source) on payments made for transfer of VDAs above ₹50,000 annually (or ₹10,000 for specific individuals).[17]

B. Regulatory Guidance from the Reserve Bank of India (RBI)

In 2018, the Reserve Bank of India (RBI) issued a circular prohibiting banks and financial institutions from providing services related to cryptocurrencies. However, in *Internet and Mobile Association of India v. Reserve Bank of India*, the Supreme Court overturned the RBI circular, finding it violative of Article 19(1)(g) of the Constitution. After the decision of the Supreme Court, the RBI decided to move to its own CBDC, i.e., the Digital Rupee (e₹), which was launched in pilot form in 2022–23. A CBDC is not a private crypto asset, but is, in essence, a legal tender backed by sovereign authority.[18]

C. Inclusion of Virtual Digital Assets under the PMLA, 2002

The Prevention of Money Laundering Act, 2002 (PMLA) has attained renewed salience with respect to digital assets, particularly cryptocurrencies and NFTs, in light of concerns about their use in crime, including terror financing, drug smuggling, ransom ware attacks, and tax evasion. In a critical development to ensure transparency and legal accountability in the digital asset ecosystem, the Ministry of Finance issued a notification on March 7, 2023, recognising that VDA transactions fall within the jurisdiction of PMLA. The notification was issued under Section 2(1)(sa)(vi) of the PMLA, making VDA service providers *Reporting Entities* under the statute.[19]

This indicates that exchanges of Indian cryptocurrency, custodial wallets, and any entity involved in the transfer, safekeeping, or management of VDAs will now be subjected to anti-AML obligations like:

1. KYC (Know Your Customer)verification,
2. Record keeping of financial transactions,
3. Suspicious transaction reporting (STR) to FIU-IND,
4. Producing information when demanded by a regulatory or investigative agency.

In its regulatory treatment of VDAs, India has adopted what commentators describe as a "mid-way" approach. Rather than either prohibiting or fully deregulating crypto-assets, the government has extended existing compliance obligations into the digital space. This is most

[16]*Income Tax Act, 1961*, § 115BBH, inserted by *Finance Act, 2022*, w.e.f. Apr. 1, 2022.
[17]*Income Tax Act, 1961*, § 194S, inserted by *Finance Act, 2022*, w.e.f. July 1, 2022.
[18]*Prevention of Money Laundering Act, 2002*, § 2(1)(sa)(vi), inserted by Ministry of Finance Notification No. S.O. 1072(E) (Mar. 7, 2023), published in *Gazette of India*, Extraordinary, Part II, § 3(ii).
[19]Reserve Bank of India, *Concept Note on Central Bank Digital Currency* (Oct. 2022), https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1218(last visited June 11, 2025).

evident from the Ministry of Finance Notification of 7 March 2023, which brought VDAs and service providers under the *Prevention of Money Laundering Act 2002*, thereby making them subject to AML and CFT requirements.[20]Similarly, the Finance Act 2022, read with provisions inserted into the *Income Tax Act 1961* (notably ss 115BBH and 194S), created a taxation framework for VDAs by imposing a flat 30% tax on income from such assets and a 1% TDS on transactions.[21] In a parliamentary response in July 2025, the Ministry of Finance clarified that crypto-assets remain "currently unregulated" but are nevertheless covered by these compliance regimes, illustrating that the state has deliberately opted for regulatory integration rather than either legalisation or prohibition.[22]Collectively, these measures represent a stepwise regulatory move that secures immediate oversight while allowing time for the government to develop more comprehensive legislation tailored to digital assets.

While this decision addresses the concerns of money laundering and terror financing, it has also increased the compliance costs imposed on Indian startups and crypto exchanges. Nevertheless, this step was a prudent compromise from a regulatory perspective, aiming to find an appropriate equilibrium between safety, innovation, and financial stability.

D. Absence of Regulation by Securities and Exchange Board of India (SEBI)

In India, although several regulators are acting upon the emergence of VDAs, the SEBI, the statutory regulator for the securities markets in India, has yet to provide comprehensive regulatory guidance aimed at Initial Coin Offerings (ICOs), Security Token Offerings (STOs), DeFi products, and similar investment-like digital product offerings. This regulatory void is in contrast to the US, where the SEC (Securities and Exchange Commission) has indicated that numerous digital tokens are securities, applying the test of whether they are offered or sold to investors.

In India, under the *Securities Contracts (Regulation) Act, 1956 (SCRA)*, the term "securities" is defined in Section 2(h) to include shares, bonds, debentures, government securities, and "any other instruments as may be declared by the Central Government."[23]The Act, however, does not explicitly indicate that digital tokens or crypto-assets would be included within its scope; nor has any notification or amendment been brought forth by the Central Government to include VDA swithin the purview of the Act. This omission creates a grey area in the Indian legal landscape. Certain VDAs like investment tokens, or DeFi products, do share attributes with traditional securities, e.g. the expectation of profit or pooling of investment, or

[20]Government of India, Ministry of Finance (Department of Revenue), Notification S.O. 1072(E), *Gazette of India*, Extraordinary, Part II, § 3(ii) (Mar. 7, 2023), https://egazette.gov.in/WriteReadData/2023/244184.pdf(last visited May 15, 2025).
[21]*Income Tax Act, 1961*, §§ 115BBH, 194S, inserted by *Finance Act, 2022*.(last visited May 24, 2025).
[22]India, Lok Sabha, Unstarred Question No. 1340, *Regulations for Virtual Digital Assets (VDA)* (answer by Minister of State for Finance Pankaj Chaudhary, July 28, 2025), https://sansad.in/getFile/loksabhaquestions/annex/185/AU1340_kPWHiB.pdf?source=pqals(last visited August 11, 2025).
[23]Securities Contracts (Regulation) Act 1956, s 2(h).

participation in the efforts of others, yet the failure to include tokens or crypto-assets under Indian securities law creates a jurisdictional ambiguity.[24]

The *"Howey Test"* is used by the SEC to ascertain whether a token is a security. Suppose the asset involves an investment of money in a common enterprise, with a reasonable expectation of profits, derived from the efforts of others. In that case, it is regarded as a security. Applying the same test to Indian crypto tokens, a significant portion of them would likely fall within the ambit of securities.

Several enforcement actions by the SEC, including high-profile cases such as *SEC v. Ripple Labs Inc.*[25] and *SEC v. Coinbase*,[26]demonstrate global trend toward classifying digital tokens functionally, regardless of their technological status. In contrast, SEBI has not publicly adopted or articulated a comparable test or framework.

E. Regulatory Position of the Reserve Bank of India (RBI)

The RBI's reaction to digital assets has transitioned from unequivocal disapproval to a more cautious approach in recent years, particularly with the evolution of the CBD Cecosystem. While the response has transitioned this far, the RBI continues to maintain a tightly constrained, risk-averse posture on VDAs, including cryptocurrencies. The RBI's discomfort with cryptocurrencies began as early as 2013, when it publicly first issued its cautionary note to consumers about the volatility, consumer protection concerns, money laundering risks, and lack of backing or intrinsic value of digital assets. RBI’s discomfort eventually resulted in the issuance of a circular dated April 6, 2018, banning all regulated entities, including banks and NBFCs, from engaging with or providing services to entities that engaged in virtual currencies. This prohibition restricted crypto exchanges from a regulated banking infrastructure and served as a de facto ban on the trading of cryptocurrencies.[27]

In 2020, however, this position was overturned in *Internet and Mobile Association of India v. Reserve Bank of India*,[28]when the Supreme Court struck down the RBI circular, ruling that the step amounted to a disproportionate restriction on the right to carry on trade or business under Article 19(1)(g) of the Constitution,and further held that in the absence of a legislative ban, such a blanket restriction could not be sustained under the RBI’s regulatory powers. Notably, in May 2021, the RBI issued a clarificatory circular stating that the 2018 circular was no longer operative due to the Court’s decision.[29]

Despite remaining antagonistic to private digital assets, the RBI proceeded to develop India’s own CBDC. The Finance Act, 2022, allowed the creation of a Digital Rupee as a form of legal

[24]Committee to Propose Specific Actions in Relation to Virtual Currencies, Ministry of Finance, Government of India, Report (2019) (Chair: Subhash Chandra Garg).
[25]*SEC v. Ripple Labs Inc.*, No. 20-CV-10832 (S.D.N.Y. 2020).
[26]*SEC v. Coinbase Global Inc.*, No. 23-CV-04738 (S.D.N.Y. 2023).
[27]Reserve Bank of India, Circular: *Prohibition on Dealing in Virtual Currencies* (Apr. 6, 2018).
[28]*Internet & Mobile Ass’n of India v. Reserve Bank of India*, (2020) 10 SCC 274.
[29]Reserve Bank of India, Circular: *Customer Due Diligence for Transactions in Virtual Currencies* (May 31, 2021).

sovereign digital currency distinct from private tokens. Section 22A of the RBI Act, 1934, was amended to permit the RBI to issue digital currency.[30]At the end of 2022 and early 2023, the RBI conducted pilot projects of the wholesale and retail CBDC, respectively. This further illustrates a 'public-private dichotomy' in India's approach, as the regulatory landscape prohibits or restricts private tokens whilst exploring state-backed alternatives.[31]

F. Attempts at Codification: The Legislative Vacuum

The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021, sought to ban private cryptocurrencies, allowing only the RBI's CBDC. However, it was never tabled, with the government citing the need for 'global consensus.'[32]

A draft law known as the Digital India Act (DIA) is set to replace the Information Technology Act, 2000, and will likely define digital assets, regulate intermediaries, and establish a regulatory sandbox for new technologies.[33]The ongoing neglect of the Indian Government to enact any digital asset legislation has resulted in a vacuum of legal certainty. Because of this, the courts and regulators are compelled to make ad hoc adjudications about legal issues associated with digital assets, resulting in compliance challenges and inhibition of India's ability to play a meaningful role in Web3 as an innovator.

COMPARING THE INDIAN REGULATORY APPROACHES TO DIGITAL ASSETS WITH THE US AND UAE

The preceding section reveals that a piecemeal approach characterises India's regulatory framework for digital assets, primarily focused on taxation and anti-money laundering measures, and marked by a legislative vacuum. While this reflects a cautious stance, it also highlights the challenges of balancing financial stability with the imperative for innovation. To draw meaningful lessons and identify potential pathways for a more coherent Indian framework, it is crucial to examine how other leading jurisdictions have navigated similar complexities. Therefore, this section undertakes a comparative study, contrasting India's regulatory position with the enforcement-led, multi-agency oversight prevalent in the US and the innovation-oriented, clarity-driven model adopted by the UAE.

A. The United States: Enforcement-Led, Multi-Agency Oversight

The regulatory framework in the US is marked by its complexity and functional approach, involving numerous federal and state authorities. A complete federal law on digital assets does not exist, but enforcement through the interpretation of existing laws serves as oversight. The primary regulatory authorities and frameworks are:

[30]*Reserve Bank of India Act, 1934*, § 22A (as amended by the Finance Act, 2022).
[31]R. Gandhi & R. Menon, Crypto and Central Banking: A Perspective from India, 58 Econ. & Pol. Wkly. 15 (2022).
[32]Vidhi Centre for Legal Policy, *Regulating Crypto-Assets in India* (2021), https://vidhilegalpolicy.in/wp-content/uploads/2021/11/Regulating-Crypto-Assets-in-India.pdf(last visited May 19, 2025).
[33]Ministry of Electronics & Information Technology (MeitY), *Concept Note on Digital India Act* (2023), https://meity.gov.in(last visited June 15, 2025).

1. Securities and exchange commission (SEC):The SEC enforces federal securities law and determines which cryptocurrencies are to be considered securities under the "Howey Test", particularly concerning ICOs and staking-as-a-service programs. The SEC's sanctions against *Ripple Labs* are noteworthy for the ramifications surrounding whether XRP is a security or not.[34]
2. Commodity futures trading commission (CFTC): The CFTC classifies certain cryptocurrencies like Bitcoin and Ethereum as commodities under the Commodity Exchange Act, thereby regulating derivatives and futures contracts on those assets.[35]
3. Financial crimes enforcement network (FinCEN):FinCEN requires cryptocurrency exchanges and wallet providers to register as Money Services Businesses (MSBs) with it and be subject to AML and reporting regulations under the Bank Secrecy Act (BSA).[36]
4. Office of the comptroller of the currency (OCC):The OCC has issued interpretive letters to federally chartered banks that allow them the privilege to custody crypto assets and to engage blockchain networks for payment settlement.[37]

B. Features:

1. Litigation-driven regulation: The regulatory environment is primarily shaped by enforcement actions and judicial decisions, creating countless variables and uncertainty for businesses operating in this domain.
2. State-level licensing: In addition to arguably excessive federal regulation, certain states like New York require companies to obtain a *Bit License*,[38]exacerbating the compliance burden.
3. Proposed legislative reforms: Several bills, such as the *Lummis-Gellibrand Responsible Financial Innovation Act (2022),*[39]seek to create a cohesive regulatory framework, but have yet to be enacted.

C. Recent Legislative Development in the United States: The GENIUS Act (2025)

A major development in the US regulatory landscape was the enactment of the *Guarding Effective National Issuance of Uniform Stable coins (GENIUS) Act,*[40] signed into law in July

[34]U.S. Securities and Exchange Commission, *Framework for "Investment Contract" Analysis of Digital Assets* (2019).
[35]In re Coinflip, Inc. d/b/a Derivabit, CFTC Docket No. 15-29 (Sept. 17, 2015).
[36]Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 9, 2019).
[37]Office of the Comptroller of the Currency, Interpretive Letter No. 1170 (July 22, 2020).
[38]N.Y. Comp. Codes R. & Regs. tit. 23, ch. I, pt. 200 (2015).
[39]Responsible Financial Innovation Act, S. 4356, 117th Cong. (2022).
[40]Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025, S. 394, 119th Cong. (2025), https://www.congress.gov/bill/119th-congress/senate-bill/394

2025. This marks the first comprehensive federal legislation specifically targeting stable coins, a category of digital assets that had previously been subject to fragmented oversight.[41]

D. Key Features of the GENIUS Act:

1. Reserve backing and transparency: All payment stable coins must be backed 100% by high-quality liquid assets. Issuers are mandated to provide monthly public disclosures of reserves, thereby ensuring transparency and accountability.[42]
2. Permitted payment stable coin issuers (PPSIs): The Act establishes a licensing regime for PPSIs, subjecting them to oversight by both federal and state regulators.[43]
3. Consumer protection and insolvency: The Act grants stable coin holders' priority in insolvency proceedings and prohibits misleading marketing claims or representations regarding asset safety.[44]
4. Regulatory coordination: The law clarifies the roles of different regulatory bodies, providing a foundation for future harmonisation across US agencies.[45]

E. Implications

The GENIUS Act marks a significant shift in the US regulatory landscape, transitioning from an enforcement-dominated model to one that incorporates targeted, asset-specific legislation. This approach blends investor protection with systemic stability while fostering innovation. For India, this development highlights the need to move beyond generic definitions and adopt asset-specific regulatory frameworks—particularly for classes such as stable coins —while also mandating transparency requirements through disclosure and reserve practices to enhance investor confidence. Equally important is the establishment of statutory mechanisms that clarify and coordinate the regulatory roles of the RBI, SEBI, and the Ministry of Finance, ensuring a coherent and unified approach to digital asset regulation.

F. United Arab Emirates: Innovation-Oriented and Regulatory Clarity

In contrast to the US, the UAE has taken a proactive and comprehensive approach to regulating digital assets. Instead of perceiving virtual assets as a risk, the country views them as a means

[41]White House, *Fact Sheet: President Donald J. Trump Signs the GENIUS Act into Law* (July 18, 2025), https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law/(last visited August 9, 2025).
[42]Simpson Thacher & Bartlett LLP, *GENIUS Act Establishes Regulatory Framework for Stablecoins* (July 22, 2025), https://www.stblaw.com/about-us/publications/view/2025/07/22/genius-act-establishes-regulatory-framework-for-stablecoins(last visited August 11, 2025).
[43]Pillsbury Winthrop Shaw Pittman LLP, *Congress Passes GENIUS Act, Establishing Framework for Stablecoin Regulation* (July 2025), https://www.pillsburylaw.com/en/news-and-insights/congress-genius-act-framework-stablecoin-digital-asset-regulation-us.html(last visited August 14, 2025).
[44]ArentFox Schiff LLP, *GENIUS Act Ushers in a New Era of U.S. Stablecoin Regulation and Digital Asset Leadership* (July 2025), https://www.afslaw.com/perspectives/alerts/genius-act-ushers-new-era-us-stablecoin-regulation-and-digital-asset-leadership(last visited August 11, 2025).
[45]KPMG, *Crypto and Digital Assets: Final GENIUS Act and Other Developments* (July 25, 2025), https://kpmg.com/us/en/articles/2025/crypto-and-digital-assets-final-genius-act-and-other-actions-reg-alert.html(last visited August 11, 2025).

to establish its technological and economic supremacy. The following are the principal legal and regulatory authorities regarding digital assets in the UAE:

1. Virtual assets regulatory authority (VARA):Established under *Dubai Law No. 4 of2022*, it regulates all crypto activities in Dubai (apart from DIFC). VARA's *Virtual Assets and Related Activities Regulations 2023* include extensive rules on licensing, custody, exchange, and token issuance for individuals and entities.[46]
2. Securities and commodities authority (SCA):Federally, SCA oversees digital asset business outside free zones, following *Cabinet Resolution No. 111 of 2022*, which imposes registration and licensure of VASPs.[47]
3. Dubai financial services authority (DFSA):DFSA regulates crypto tokens under the *Crypto Token Regulatory Framework 2022* with a focus on governance, investor protection, and cybersecurity.[48]

G. Features:

1. Clear asset classification: Crypto assets are categorised into payment tokens, security tokens, and utility tokens, with separate treatment and compliance standards.
2. Attracting investment: Businesses like *Binance* and *Crypto.com* have been authorised under this framework, which shows international investor trust.
3. FATF alignment: Although the UAE was placed on the FATF grey list in 2022, it has taken strong steps to enhance its AML/CFT supervision, particularly concerning VASP s and cross-border crypto flows.

The preceding detailed examination of regulatory frameworks in India, the US, and the UAE reveals a clear divergence in strategic approaches to digital assets. From India's cautious and fragmented stance to the US's litigation-driven oversight and the UAE's proactive, innovation-friendly model, each jurisdiction presents unique lessons. To consolidate these insights and visually articulate the key differences and commonalities in their respective regulatory philosophies, the following comparative matrix systematically outlines the core features, challenges, and strengths of each approach.

COMPARATIVE MATRIX: US, UAE AND INDIA

While India is cautious, the UAE has established itself as a world leader, and the US, until recently, trailed behind with a fragmented regulatory landscape and perpetual court tussles. Today, India is more focused on tax compliance and anti-money laundering requirements, not encouraging innovation or acknowledging the multi-asset nature of digital assets. In contrast, the UAE's transparency, forward-thinking regulations, and investor-friendly systems have positioned it as a top jurisdiction for crypto-based entrepreneurship. India can learn from both jurisdictions by incorporating the UAE's model of classification and licensing, and the investor

[46]Virtual Assets Regulatory Authority (VARA), *Virtual Assets and Related Activities Regulations 2023* (Gov't of Dubai, 2023).
[47]Cabinet Decision No. 111 of 2022 Concerning the Regulation of Virtual Assets and Their Service Providers (U.A.E.).
[48]Dubai Financial Services Authority (DFSA), *Crypto Token Regulatory Framework* (2022).

protection principles adopted by the US, while developing a context-specific, innovation-friendly regulatory regime.

The recent enactment of the *GENIUS Act* in the US provides an additional comparative lesson. Unlike the earlier fragmented enforcement-dominated model, this Act marks a decisive move towards asset-specific legislation, particularly in relation to stablecoins. By combining investor protection, transparency, and systemic stability with an enabling approach to innovation, the Act demonstrates the possibility of balancing regulation with growth. For India, this underscores the importance of moving beyond generic definitions, developing targeted frameworks for different categories of digital assets, and ensuring coordinated oversight between the RBI, SEBI, and the Ministry of Finance.

CONCLUSION

The advent of digital assets represents a structural shift in the global financial system, sparking difficult questions of technology, law, and policy. India has responded with needed early action through its tax and anti-money laundering laws; however, its regulatory framework remains mostly reactive, piecemeal, and poorly calibrated to the technological dynamism of virtual digital assets. In contrast, the US (enforcement-led regulation) and the UAE (innovation-led regulation) provide useful models. The recent enactment of the *GENIUS Act* in the US further reflects a decisive move towards asset-specific legislation, particularly in relation to stable coins, marking a major shift away from a purely enforcement-led approach. Their experience indicates the importance of a clear classification of the asset, coordination among regulators, and legal certainty. India finds itself at a regulatory inflexion point. Taxation alone, without a supporting regulatory framework, risks driving innovation abroad and limiting the potential of the digital asset ecosystem. A coherent digital asset framework has undoubtedly stifled innovation, investor confidence, and institutional participation. But this scenario also represents an opportunity to look forward, and to come up with a balanced and innovation-supportive regime that protects financial stability without strangling the technology.

As the ecosystem around digital assets evolves, India's regulatory approach must be guided by clarity, flexibility, and foresight. While opting for the adoption of best international practices, India can build a regime on its own economic and legal realities and thus emerge not merely as a passive bystander but as a global observer of thought in the digital asset regulation. This necessitates coordination between the RBI, SEBI, and the Ministry of Finance to avoid jurisdictional overlap and to ensure systemic stability. Albeit the path forward will not be easy, with sound policymaking and stakeholder engagement, India stands poised to craft a digital asset framework that balances innovation with responsibility — a balance that will ultimately determine whether it is a follower in the global order or a leader in it.

BALANCING INNOVATION AND PROTECTION: A CRITICAL EXAMINATION OF INDIA'S LEGAL FRAMEWORK GOVERNING CYBERSECURITY AND DATA PRIVACY IN VIRTUAL DIGITAL ASSET TRANSACTIONS

Prishima K
Student
SASTRA Deemed University
Thanjavur, Tamil Nadu

N. Prabhavathi
Assistant Professor
SASTRA Deemed University
Thanjavur, Tamil Nadu

Abstract

The rapid expansion of Virtual Digital Assets (VDAs), including cryptocurrencies, non-fungible tokens, and blockchain-based digital assets, has significantly reshaped India's financial ecosystem by fostering technological innovation while simultaneously intensifying cybersecurity and personal data protection risks. Despite increased adoption and partial regulatory recognition, India's legal framework governing VDAs remains fragmented, relying on general statutes such as the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and sector-specific advisories issued by the Reserve Bank of India and the Securities and Exchange Board of India. These instruments inadequately address blockchain-specific characteristics such as decentralization, pseudonymity, and immutability, which challenge traditional data protection principles. This study critically examines the effectiveness of India's existing legal and institutional mechanisms in regulating cybersecurity and privacy risks associated with VDA transactions. Employing a doctrinal and analytical research methodology, the paper analyzes statutory provisions, regulatory practices, judicial developments, and comparative international frameworks. The study identifies significant regulatory gaps in cybersecurity standards, investor protection, and inter-agency coordination, concluding that India requires a unified, innovation-friendly regulatory framework that integrates data protection, cybersecurity, and consumer safeguards to ensure sustainable growth of the VDA ecosystem.

Key Words: Blockchain Governance, Personal Data Protection, Investor Protection, Financial Technology Law, privacy-preserving technologies

1. INTRODUCTION

India's digital economy is fast changing with the rapid adoption of Virtual Digital Assets, which include everything from cryptocurrencies and NFTs to blockchain-based tokens and decentralised finance applications. At its very core, this revolution has been driven by blockchain technology, whose inherent qualities of decentralisation, immutability, and transparency have challenged conventional notions regarding asset ownership, financial settlement, and regulation. It is these disruptive qualities of VDAs that have allowed Indian users to seek new avenues for investment, raise funds, and achieve digital innovation, while simultaneously causing friction in traditional notions of financial and legal accountability.

Over the past few years, India's digital asset ecosystem has experienced exponential growth. Government recognition of VDAs, as represented by their classification and taxation under the Finance Act, 2022, has catalysed the proliferation of domestic exchanges, platforms, and fintech startups focused on crypto-asset trading and development. Already, the burgeoning ecosystem no longer caters to a niche demographic; millions of retail investors are involved, with diverse technological and entrepreneurial activities stimulated. However, regulatory clarity and investor confidence remain hamstrung by fragmented laws and sector-specific guidelines, unable to keep pace with the transnational, pseudonymous nature of blockchain-driven innovation. With these developments, the requirement for dedicated cybersecurity and privacy regulation has increased manifold. The very fundamental architecture of blockchain, while resistant to tampering and censorship, poses new and acute risks: sophisticated cyberattacks, data breaches, phishing scams, and ransomware incidents affecting exchanges and wallets; likewise, the pseudonymity and immutability of records on the blockchain complicate the application of rights and obligations central to Indian data protection laws on consent, the right to erasure, and the accountability of data fiduciaries under the Digital Personal Data Protection Act, 2023. In the absence of a consistent legal framework for addressing these concerns, users and investors, along with service providers, remain exposed in an ecosystem in which technological development is outpacing statutory innovation.

2. REVIEW OF LITERATU[1]RE

Scholarly discourse on Virtual Digital Assets (VDAs) has expanded significantly in recent years, particularly in response to the rapid proliferation of cryptocurrencies, blockchain-based platforms, and decentralized financial systems. Early literature primarily examined VDAs through the lens of economic regulation and monetary policy, focusing on concerns relating to financial stability, systemic risk, and illicit financial flows. Indian academic commentary

[1] Reserve Bank of India, Statement on Developmental and Regulatory Policies (2018).
2 Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 274.
3 Finance Act, 2022.
4 Digital Personal Data Protection Act, 2023
5 Academic commentary on blockchain immutability and data protection.
6 CERT-In Directions, April 28, 2022
7 Cybersecurity literature on crypto platforms.

in this phase largely reflected regulatory apprehension, particularly following the Reserve Bank of India's restrictive stance prior to 2020. [1] However, this body of work paid limited attention to cybersecurity vulnerabilities and personal data protection risks inherent in blockchain-based transactions. After the Supreme Court's decision in Internet and Mobile Association of India v. Reserve Bank of India (2020), scholarly analyses began to shift towards regulatory proportionality and innovation-friendly governance.[2] Legal scholars observed that while the judgment curtailed excessive regulatory prohibition, it did not establish a comprehensive framework for governing VDAs. Subsequent literature critically evaluated India's approach of recognizing VDAs for taxation purposes under the Finance Act, 2022, arguing that fiscal recognition without parallel development of cybersecurity and consumer protection standards resulted in a fragmented regulatory ecosystem. [3] Another significant strand of literature examines India's evolving data protection regime, particularly following the enactment of the Digital Personal Data Protection Act, 2023. Commentators acknowledge that the Act introduces a consent-based data governance framework and codifies rights such as access, correction, and erasure. [4] However, scholars critically argue that the DPDP Act is structurally designed for centralized data controllers and does not sufficiently accommodate decentralized blockchain architectures.[5] Cybersecurity-focused literature on VDAs predominantly addresses technological risks associated with exchange hacks, wallet breaches, phishing attacks, and ransomware payments. Studies analyzing CERT-In's incident reporting directions recognize the inclusion of VDA-related cyber incidents within India's cybersecurity governance framework. Nevertheless, scholars criticize the absence of VDA-specific cybersecurity standards. [7]
International literature offers valuable comparative insights, particularly the EU's Markets in Crypto-Assets (MiCA) Regulation and Singapore's Payment Services Act, which provide integrated models combining cybersecurity, consumer protection, and regulatory oversight.[8 9]
A critical gap emerging from the reviewed literature is the absence of an integrated analysis examining cybersecurity, data protection, and institutional governance of VDAs within the Indian context. Accordingly, the present study seeks to bridge this gap.

3. RESEARCH OBJECTIVES

1. To examine India's existing legal framework governing cybersecurity and data privacy in VDA transactions.
2. To identify regulatory and institutional gaps arising from blockchain-specific characteristics.
3. To assess the effectiveness of current compliance and enforcement mechanisms.
4. To analyse international regulatory models governing VDAs.
5. To propose reforms balancing innovation with investor and consumer protection.

4. RESEARCH QUESTIONS

RQ1: To what extent do India's current laws regulate cybersecurity and privacy risks in VDA transactions?
RQ2: What legal and institutional reforms are required to establish a balanced and innovation-friendly VDA regulatory regime?

5. RESEARCH METHODOLOGY

The present study adopts a doctrinal and analytical research methodology, relying exclusively on secondary sources of data. The doctrinal method is employed to examine and interpret existing legal frameworks governing Virtual Digital Assets (VDAs), cybersecurity, and data protection in India. This includes a systematic analysis of statutory provisions such as the Finance Act, 2022, the Digital Personal Data Protection Act, 2023, relevant Information Technology laws, CERT-In directions, and regulatory guidelines issued by competent authorities. [8] [9] [2]

Judicial decisions of the Supreme Court of India and other relevant forums are analysed to understand the evolving judicial approach towards VDAs, regulatory proportionality, and digital rights. Particular emphasis is placed on landmark judgments shaping the legal status of cryptocurrencies and the balance between innovation, regulation, and individual rights. The analytical method is further applied to critically evaluate regulatory gaps, inconsistencies, and enforcement challenges relating to cybersecurity and data privacy in VDA transactions. Comparative analysis forms a supplementary component of this study, wherein select international regulatory frameworks—such as the European Union's Markets in Crypto-Assets (MiCA) Regulation and Singapore's Payment Services Act—are examined to identify best practices relevant to the Indian context. Secondary sources including books, peer-reviewed journal articles, policy papers, reports of international organisations, and official government publications are utilised to support doctrinal interpretation and critical analysis. The study does not involve empirical data collection and is limited to qualitative legal analysis. Through this methodology, the research aims to develop a coherent understanding of the existing regulatory framework and propose informed suggestions for strengthening cybersecurity and data protection governance of VDAs in India.

6. DATA ANALYSIS AND INTERPRETATION:

The data gathered from secondary sources were analyzed using a qualitative thematic analysis technique. The technique enabled the retrieval and interpretation of themes arising from statutes, judicial pronouncements, policies, and scholarly discourse regarding Virtual Digital Assets (VDA) law. These themes were interpreted under a set of themes that ensured a systematic interpretation.

Theme I: Recognition of Regulation Without Comprehensive Governance:

It can be observed from the analysis that there has been a partial regulatory recognition of VDAs by the Indian government, especially in terms of taxation and compliance requirements. The lack of a comprehensive regulatory framework covering cybersecurity and data protection obligations has led to the uncertainties in the regulations in the country.

[2] [8] Regulation (EU) 2023/1114 (MiCA).

[9] Singapore Payment Services Act, 2019.

Theme II: Risks of Cybersecurity in VDA Transactions:

The literature on law and policy has identified the elevated cybersecurity risk associated with VDA platforms as one of the themes. The threats of hacks on exchanges, personal keys, phishing attacks, and smart contract vulnerabilities pose serious financial and data risks to users.

Theme III: Data Privacy Challenges in Decentralized Systems:

The paper points out the difficulties associated with the applicability of conventional data protection rules to blockchain systems. Consistency with rules on consent, data minimisation, or the right to be forgotten is, in practice, impossible. This is attributed to the immutable nature of the blockchain.

Theme IV: Institutional and Regulatory Fragmentation:

It is clear from the analysis that the regulation of cyber issues is fragmented, involving more than one authority, and the enforcement authority is ambiguous and ineffective in responding to cyber attacks and breaches of data in VDA transactions.

Theme V: Insights from Comparative Regulation:

From comparative analysis, regimes like the European Union and Singapore have taken up an integrated approach to regulation that harmonizes financial regulation, cybersecurity compliance, and data protection, providing a learning experience for India too.

Interpretation:

There are apparent discrepancies in Indian law regarding VDA regulation between what is practiced in India and what has been recommended based on international standards and guidelines related to data protection in emerging sectors like VDAs or a similar emerging technology-driven sector. The thematic findings indicate that there are no convergent regulatory strategies between controlling finance and managing cybersecurity and data.

7. CONCEPTUAL FRAMEWORK

Virtual Digital Assets are a broad class of digital representations of value enabled by blockchain and DLT. Commonly, such assets are grouped into various types, including but not limited to cryptocurrencies, NFTs, utility tokens, security tokens, and stablecoins, for serving different

purposes within digital ecosystems. The most prominent of these, of course, are cryptocurrencies like Bitcoin and Ethereum, truly acting as mediums of exchange or stores of value. Then there are NFTs, which are unique digital ownership rights to art, music, and other collectibles, distinguished because they are non-fungible. Utility tokens grant access to specific services or resources available on blockchain platforms, while security tokens

generally represent investment contracts or equity and thus are designed to be compatible with regulatory requirements.

In order to understand the operational dynamics and legal inferences of VDAs, it is important to investigate blockchain technology in itself. Blockchain is a distributed, peer-to-peer network that records transactions across various nodes. Because of cryptographic and consensus mechanisms, tampering with data becomes highly impractical. Decentralization eliminates a central authority, which makes such mechanisms resilient and more transparent but also difficult to regulate. Pseudonymity is one of the core features: instead of identifiable personal data, users communicate via cryptographic addresses. This entails increased privacy of users but simultaneously makes illicit activities such as money laundering and fraud easier. Transactions, once validated, are irreversibly recorded, and this concept is called immutability. Immutability assures data integrity, yet it poses considerable problems for privacy rights, particularly regarding the right to erasure under data protection laws on data. The concerns for cybersecurity and data protection in VDA-related transactions are several. The open, borderless nature of a blockchain network exposes its participants a targeted cyberattacks, including hacking of exchanges, wallet breaches, and dissemination of malware.

Such exchange hacks have indeed led to substantial losses among investors, demonstrating the vulnerabilities in the technical infrastructure and operational security protocols. The pseudonymous nature of blockchain transactions further undermines effective regulation and forensic investigation, while increasing user privacy. The irreversibility and immutability of blockchain data go against data privacy principles like the right to be forgotten, thereby raising several legal concerns pertaining to consent and data minimisation. In fact, India's entire digital asset ecosystem, while nascent and ever-growing, does need an all-inclusive cybersecurity and privacy regime to protect its citizens and preserve trust in these emerging technology areas where regulatory authorities are struggling to make a perfect balance between innovation and security.

8. THE INDIAN LEGAL AND REGULATORY FRAMEWORK

The legal architecture for VDAs in India is currently distributed across general cyber law under the Information Technology Act, 2000, and CERT-In directions; the data protection regime under the Digital Personal Data Protection Act, 2023; and financial sector oversight and advisories by the RBI and the Securities and Exchange Board of India, creating thus a patchwork rather than a single VDA-specific statute. While the DPDP Act codifies consent-based processing, rights of access, correction, and erasure, and provides for a special Data Protection Board, it follows a "negative list" approach to cross-border transfers by allowing transfers by default, except to countries the government may notify as restricted, with sectoral rules applying where they provide higher safeguards. In the governance of cyberspace, CERT-In's April 2022 Directions mandate incident reporting within six hours of noticing an incident, explicitly bringing within the reportable taxonomy incidents affecting blockchain, virtual assets, exchanges, and custodian wallets, thereby increasing technical and organizational security requirements for digital asset intermediaries and their service providers. The RBI prohibited regulated entities on April 6, 2018, from dealing in or

facilitating virtual currency activity, which was set aside by the Supreme Court in 2020 in Internet and *Mobile Association of India v. RBI* on the ground that it was disproportionate. Thereafter, in May 2021, the RBI clarified that banks need not refer to the quashed circular but must continue to apply basic due diligence standards, thus indicating risk-based supervision without a blanket ban. SEBI, though not notified as the sectoral regulator for crypto-assets, has strengthened market-wide cyber governance through circulars on Cyber Security and Cyber Resilience for regulated entities and portfolio managers, which could be read as reference benchmarks for any tokenized securities or VDA-adjacent market infrastructure falling within the securities perimeter. Taxation and compliance measures have advanced faster than sector-specific prudential regulation, with the Finance Act, 2022, inserting section 115BBH to tax income from the transfer of VDAs at a flat 30% without set-off (other than cost of acquisition) and introducing section 194S to require 1% TDS on consideration for transfer, thereby institutionalizing reporting and collection at source across the VDA lifecycle. In parallel, the Ministry of Finance notified, in March 2023, that VDA service providers fall within the ambit of "reporting entities" under the Prevention of Money Laundering Act, 2002, obligating exchanges, custodians and transfer services onshore and offshore dealing with India-facing activity to register with FIU-IND, implement KYC, maintain records and file suspicious transaction reports under an activity-based approach. with public communications underscoring that crypto products and NFTs remain unregulated and risky from a consumer recourse standpoint. For data protection compliance, the DPDP Act's duties for data fiduciaries and processors now form the primary personal data regime, while sectoral data-localization directives (e.g., RBI's payment data circular) continue to override where stricter, and CERT-In's breach-reporting and log-retention directives impose additional technical accountability layers relevant to Indian VDA platforms and service vendors. In combination, these taxes, AML/CFT, and data-governance obligations impose substantive compliance expectations on Indian VDA intermediaries, even as a bespoke prudential or conduct code for VDAs is yet to be enacted. Significant overlaps and gaps persist due to multi-agency touchpoints and the absence of a single accountable regulator for VDAs, producing jurisdictional ambiguity among RBI (financial stability and payments), SEBI (securities market integrity), MeitY/CERT-In (cybersecurity), and the DPDP Board (personal data), with sectoral rules prevailing over privacy rules where they are stricter. A structure that can both protect sensitive financial data and fragment compliance pathways for VDA businesses.

While taxation and AML rules are relatively clear, consumer and investor protection for VDAs remains "unregulated," as publicly noted by the government, reflecting a gap between fiscal and crime-control measures on one hand and prudential, conduct, custody, and cybersecurity standards tailored to VDAs on the other. Cross-border enforcement complicates matters further: the PMLA's activity-based, extraterritorial registration requirement seeks to bring offshore platforms within FIU oversight, while the DPDP Act's negative-list model for international transfers leaves operational uncertainty pending notifications, and CERT-In's six-hour reporting can be operationally burdensome for globally distributed exchanges reliant on third-country infrastructure. Finally, although SEBI has strengthened cyber resilience for entities it regulates, the lack of a VDA-specific cyber standard covering hot/cold wallet management, key custody, and incident disclosure for exchanges and custodians creates a

regulatory lacuna that is only partially addressed by generic CERT-In directions and sector-agnostic privacy obligations. [11]

9. PRIVACY AND CYBERSECURITY GAPS

One of the foremost challenges in regulating Virtual Digital Assets (VDAs) lies in the conflict between blockchain's inherent immutability and established privacy principles. Blockchain's foundational characteristic is that transaction data once recorded cannot be altered or deleted directly conflicts with privacy rights such as the "right to be forgotten" and data erasure obligations embedded in data protection regimes like India's Digital Personal Data Protection Act, 2023. This immutability complicates user control over personal data and challenges the conventional consent-based framework, which relies on the ability to modify or delete sensitive information upon request. Emerging technical approaches like off-chain data storage, zero-knowledge proofs, and privacy-preserving smart contracts offer potential solutions but remain largely experimental and have not been integrated into mainstream Indian regulatory policies.

Cybersecurity risks present another significant gap. The VDA ecosystem has been plagued by high-profile cyberattacks targeting cryptocurrency exchanges, wallet providers, and associated infrastructure. These breaches often result from poor key management, software vulnerabilities, insider threats, and inadequate regulatory oversight. Indian exchanges have suffered from hacks resulting in multi-crore losses, revealing systemic weaknesses in technical safeguards and incident preparedness. The pseudonymous nature of blockchain, while enhancing privacy, also facilitates money laundering, fraud, and ransomware payments, hindering effective law enforcement and regulatory intervention. Despite CERT-In's stringent incident reporting directives, the absence of prescriptive cybersecurity standards specifically tailored for VDA platforms, such as secure wallet custody protocols and transaction monitoring, leaves Indian users exposed to risks. The gap is exacerbated by the cross-border nature of the technology, complicating enforcement and incident response.[3]

10. COMPARATIVE AND INTERNATIONAL PERSPECTIVE

The European Union's Markets in Crypto-Assets (MiCA) Regulation, coupled with the General Data Protection Regulation (GDPR), represents a comprehensive integrated approach to regulating VDAs with a dual focus on market integrity and privacy protection. MiCA introduces harmonised licensing, operational, and transparency requirements for crypto-asset issuers and service providers, including cybersecurity obligations and consumer protection norms. GDPR's stringent data protection principles, such as data minimisation, purpose limitation, and cross-border data transfer restrictions, are clearly articulated and enforceable, setting a high benchmark for privacy compliance in the digital asset sector. This synergy ensures that VDAs operate within a robust regulatory ecosystem, balancing innovation with strong user protections. Singapore's Payment Services Act (PSA) exemplifies a risk-based

[3] Press Information Bureau, "FIU-IND Issues Notices to 25 Offshore Virtual Digital Asset Service Providers" (Oct. 2, 2025), available at https://www.pib.gov.in/PressReleasePage.aspx?PRID=2173758

regulatory framework that standardizes licensing requirements according to the type and risk profile of digital payment services, including VDAs. The PSA mandates strong anti-money laundering (AML) controls, customer due diligence, safeguarding of client funds, and operational resilience. Singapore's approach prioritizes regulatory flexibility by enabling innovation through sandboxes and fostering public-private dialogue, while ensuring that service providers maintain adequate cybersecurity and compliance standards. This calibrated regulation differentiates Singapore as a leading global hub for responsible digital asset innovation.

Globally recognized standards such as the Financial Action Task Force (FATF) guidelines on Virtual Asset Service Providers (VASPs) have significantly influenced countries' regulatory frameworks. FATF mandates registration, AML/KYC protocols, transaction record-keeping, and suspicious activity reporting for VASPs. These recommendations are designed to mitigate the risks of money laundering and terrorist financing via virtual assets. India has taken steps to align with FATF standards, particularly by mandating VDA service provider registration with the Financial Intelligence Unit (FIU-IND), and implementing reporting and KYC norms, although implementation across the decentralized, global VDA ecosystem remains inconsistent. Challenges in enforcement and cross-border data transfers arise primarily due to the borderless, decentralized nature of VDAs. Jurisdictional ambiguities, data localization norms, and differing international standards impede effective cooperation among regulators and law enforcement agencies. While India's DPDP Act adopts a default-permission approach to cross-border data transfer with exceptions for notified countries, the [4]

operationalization of these provisions for VDAs, which often involve distributed nodes and global actors, is complex. The absence of harmonized international regulatory cooperation further complicates timely investigation and response to cybercrime and fraud in the VDA space, requiring enhanced bilateral and multilateral engagements for regulatory convergence and mutual legal assistance.[12]

11. BALANCING INNOVATION AND REGULATION

In recognition of the rapidly evolving Virtual Digital Asset (VDA) landscape, regulatory sandboxes have emerged as crucial instruments for fostering innovation while maintaining oversight. Indian regulators like RBI, SEBI, and IFSCA have operationalised sandbox frameworks to allow fintech and blockchain-based solutions to be tested in controlled environments, enabling the identification and mitigation of risks before full-scale deployment. These sandboxes encourage collaborative dialogue between innovators and regulators, helping refine regulatory approaches without stifling technological advancement. Complementing this, self-regulation models promoted by industry bodies can deliver adaptable operational standards, increase compliance culture, and facilitate rapid response to

[4] 12 Harsh Awasthi, *Taxation of Cryptocurrency & Virtual Digital Assets (VDAs): Sections 115BBH & 194S – Understanding Method of Taxation*, TaxGuru (Aug. 25, 2025),
13 **Crypto Taxation in the Finance Act, 2022 (The Indian Conundrum)**, L&S Insights (Apr. 19, 2022), https://lakshmisri.com/insights/articles/crypto-taxation-in-the-finance-act-2022-the-indian-conundrum

emerging threats, although they require strong regulatory backstops to prevent consumer harm.[13]

Privacy by design has become a central principle in aligning blockchain and data protection objectives. Integrating privacy-preserving technologies such as zero-knowledge proofs, encryption, and off-chain storage mechanisms enables compliance with data protection mandates like consent management and the right to erasure, despite blockchain's immutable nature. Technical compliance mechanisms, including robust key management, secure wallet architecture, transaction anomaly detection, and automated breach reporting protocols, are essential for elevating cybersecurity standards specifically tailored for VDAs. Policy recommendations for harmonized governance urge the consolidation of VDA regulation under a unified statutory framework that integrates data protection, cybersecurity, taxation, and conduct regulation. This framework should establish clear licensing, operational, and consumer protection standards, harmonizing divergent rules from RBI, SEBI, MeitY, and the DPDP Board. Enhancing cross-agency coordination via a central VDA regulatory authority or inter-agency task force would streamline enforcement and reduce jurisdictional conflicts. Further, the adoption of international best practices such as those from the EU's MiCA Regulation and Singapore's Payment Services Act tailored to India's socio-economic context,[5] can provide balanced regulation fostering innovation, protecting consumers, and ensuring systemic stability.

12. INSTITUTIONAL AND REGULATORY CHALLENGES IN VIRTUAL ASSET LANDSCAPE

The regulatory and institutional environment governing Virtual Digital Assets (VDAs) in India exhibits multilayered complexities arising from overlapping jurisdictions, evolving policies, and the inherent technological novelties of blockchain-based assets. This chapter provides a comprehensive analysis of the institutional architecture currently impacting VDAs, spotlighting the challenges posed by regulatory fragmentation, enforcement hurdles, and the need for coherent governance to support the sustainable growth of India's VDA ecosystem. At present, India's VDA sector is influenced by multiple agencies, including the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Ministry of Electronics and Information Technology (MeitY), the Data Protection Board constituted under the Digital Personal Data Protection Act, 2023, and the Financial Intelligence Unit – India (FIU-IND). [10]

Each institution brings a sectoral focus aimed at addressing specific risks: RBI focuses primarily on financial stability and payment systems; SEBI targets securities and market integrity; MeitY oversees cyber and data frameworks; FIU-IND enforces anti-money laundering (AML) requirements; and the Data Protection Board governs personal data compliance. However, this multi-agency polycentricity generates coordination challenges,

[5] 10. Income-tax Act, 1961, No. 43 of 1961 (India).
14. Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India) (enacted Aug. 11, 2023), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

regulatory overlaps, and jurisdictional ambiguities, amplifying complexity for stakeholders and complicating enforcement efficacy. [14]

One key institutional challenge is the lack of a single designated regulatory authority with a clear mandate over VDAs. Unlike jurisdictions such as Singapore, where a unified regulatory framework under the Payment Services Act consolidates oversight, India's sector-wise approach leads to inconsistent risk assessment criteria and fragmented regulatory treatment. For example, while RBI historically issued prohibitive circulars against cryptocurrency dealings, the Supreme Court's 2020 judgment scaled back this stance, prompting RBI to adopt a more calibrated supervisory approach, yet ,absent clear statutory backing, the delineation of regulatory roles remains uncertain. SEBI has begun extending its cybersecurity and cyber resilience frameworks to tokenized securitie,s but stops short of unequivocally classifying most VDAs as securities, limiting its supervisory reach. Meanwhile, MeitY's Cyber Emergency Response Team-India

(CERT-In) has issued mandatory incident reporting directives, but these apply broadly without VDA-specific tailoring. FIU-IND enforces robust AML/KYC compliance but lacks consumer protection or innovation-fostering roles.

The interagency coordination deficit manifests in practical enforcement issues. Disparate regulatory standards create compliance inefficiencies for VDA service providers, with overlapping audit requirements, gaps in data protection protocols, and conflicting governance obligations. This mismatch risks regulatory arbitrage, where entities may segregate activities to align with the least stringent regulator, undermining systemic safeguards. Furthermore, the rapid evolution of decentralized finance (DeFi) protocols further strains the institutional framework. DeFi's automated, smart contract-based operations challenge traditional regulatory models predicated on identifiable intermediaries, raising critical questions on accountability, regulatory reach, and investor protection. Absence of clear policy on DeFi governance increases investor vulnerability and inhibits effective enforcement.

In response, recent policy discussions emphasize the need for an overarching coordination mechanism or a dedicated Virtual Digital Asset Regulatory Authority (VDARA) to streamline rulemaking, licensing, supervision, and consumer redress across agencies. Such an entity could institutionalize knowledge sharing, unify market conduct standards, and serve as a single point for industry engagement and compliance oversight. Additionally, integration of

Technology-enabled regulatory approaches (RegTech and SupTech) can enhance real-time monitoring and risk assessment while facilitating regulatory innovation and sandboxing. Establishing clear legal definitions and taxonomies for VDAs and VASP activities, harmonizing reporting obligations, and clarifying jurisdictional parameters remain foundational for regulatory coherence. Institutional reforms must also incorporate stakeholder empowerment through capacity building, awareness programs, and dispute resolution frameworks to bolster user confidence and market transparency. Public-private partnerships can stimulate standards development, cybersecurity best practices adoption, and privacy-by-design innovations, ensuring regulatory measures align with technological realities and market needs.

In conclusion, while India has made significant strides in incorporating VDAs within its existing regulatory umbrella, institutional fragmentation and policy ambiguity threaten to undermine regulatory effectiveness and sectoral growth. A holistic, institutionally integrated model coupled with adaptive regulatory tools and clear statutory mandates is imperative to reconcile innovation with investor protection, data privacy, and cybersecurity imperatives in India's emerging digital asset economy.

13. NAVIGATING COMPLIANCE AND ENFORCEMENT CHALLENGES IN INDIA

The regulatory journey of Virtual Digital Assets (VDAs) in India reflects a complex evolution amid rapid technological innovation and regulatory gaps that demand urgent harmonization. Although India has yet to enact a comprehensive VDA-specific legislation, piecemeal developments ranging from sectoral guidelines to taxation and anti-money laundering rules have laid a patchwork legal fabric regulating certain facets of the ecosystem.

This chapter delves into the intricate compliance and enforcement challenges faced by Indian regulators and market participants, focusing on standards-setting, regulatory clarity, and enforcement operations while highlighting the tensions between innovation, consumer protection, and systemic integrity.

India's foundational recognition of VDAs came through the Finance Act, 2022, which introduced a direct taxation regime for income earned through the transfer of VDAs, imposing a flat 30% tax alongside 1% TDS on transaction consideration. This fiscal codification was supplemented by the Ministry of Finance's notification bringing Virtual Digital Asset Service Providers (VASPs) including exchanges, custodians, and wallet services under the ambit of the Prevention of Money Laundering Act (PMLA), mandating stringent KYC (Know Your Customer) and AML (Anti-Money Laundering) compliance as well as registration with the Financial Intelligence Unit of India (FIU-IND). The FIU-IND has emerged as a pivotal de facto regulator in the absence of a dedicated VDA regulator, assuming oversight responsibilities primarily for financial crimes, but its regulatory jurisdiction does not extend comprehensively into consumer protection, cybersecurity, or innovation facilitation.This dual compliance environment has posed significant operational burdens on VDA platforms.

Exchanges, both domestic and offshore, are now compelled to regularly submit detailed compliance reports, maintain robust audit trails, and enforce prudent operational controls to mitigate risks of fraud, money laundering, and market abuse. Notably, FIU-IND has taken decisive enforcement action against non-compliant platforms by issuing show-cause notices and instituting penalties for violations of PMLA obligations, including KYC lapses and lack of registration, evidencing a robust regulatory intent to check illicit activities in the sector.

However, enforcement remains a challenge due to the decentralized, borderless nature of many VDAs and DeFi (Decentralized Finance) platforms, where traditional points of control and regulatory touchpoints are blurred.

A significant compliance challenge stems from the legal and operational treatment of DeFi protocols within India's regulatory framework. Although the law does not offer explicit exemptions for DeFi, the practical applicability of VASP obligations depends on the degree of decentralization demonstrated by the protocol. Many DeFi projects exist on a spectrum, from centrally governed to fully decentralized models, requiring nuanced regulatory calibration. For example, DeFi protocols with administrator keys or custodial functions arguably fall within the VASP regulatory perimeter, while fully autonomous smart contracts may escape direct oversight, posing potential gaps in consumer protection and AML enforcement.

Cybersecurity remains a foundational pillar of regulatory concern, paralleling financial compliance. The Ministry of Electronics and Information Technology (MeitY) and CERT-In have augmented incident reporting requirements for entities engaged in VDA-related activities, mandating incident disclosure within tight timeframes to promptly address cyber threats. Further, the Securities and Exchange Board of India (SEBI) and Reserve Bank of India (RBI) have issued specialized guidelines enhancing cyber resilience and risk management standards, particularly for intermediaries dealing in tokenized securities or providing banking services to crypto businesses. These moves mark recognition that safeguarding VDA infrastructure is essential to maintain market integrity and investor confidence. [15]

Amidst existing frameworks and enforcement activity, India's approach continues to evolve with an emphasis on risk-based regulation and innovation facilitation. Regulatory sandboxes enable market players to test novel VDA products under regulatory supervision, allowing regulators to gather data to inform policymaking without unduly stifling innovation. The RBI's 2025 Crypto Framework embodies this ethos by introducing tiered operational permissions for regulated entities, balancing innovation support with consumer safeguards. Finally, India's proactive alignment with international frameworks such as the FATF guidelines on VASPs signals its commitment to global standards while adapting to the domestic context, reinforcing accountability through transparency obligations and cross-border cooperation mechanisms. In conclusion, the enforcement and compliance landscape for VDAs in India is characterized by a dynamic but fragmented regime, which has made significant strides in financial compliance and cyber risk mitigation but still faces challenges related to regulatory clarity, decentralized finance, and technological advancement. A dedicated, comprehensive regulatory framework, coupled with enhanced cross-agency coordination and technological adoption, is vital to harmonize these competing imperatives and position India as a robust, innovation-friendly hub for virtual digital assets.

14. ADDRESSING LEGAL AND ETHICAL CHALLENGES IN CONSUMER PROTECTION AND INVESTOR SAFEGUARDS:

The rapid proliferation of Virtual Digital Assets (VDAs) in India's financial ecosystem has raised pressing legal and ethical questions regarding consumer protection and investor safeguards.

Despite significant market interest and growth, the absence of a comprehensive regulatory regime has led to increased exposure of retail investors to fraud, misinformation, market manipulation, and inadequate redress mechanisms. This chapter critically examines the

challenges inherent in protecting consumers in the VDA sector, analyzes the legal instruments currently available, and proposes a framework for robust investor protection [6]aligned with ethical governance principles. India's VDA market is characterized by a predominance of retail participation, often driven by speculative motivations and limited understanding of underlying technological risks. The lack of tailored disclosure requirements and the opaque nature of many VDA products create asymmetries in information, enabling malpractices including pump-and-dump schemes, fake Initial Coin Offerings (ICOs), and Ponzi operations. The absence of a statutory definition clearly distinguishing securities from other digital tokens complicates the application of extant investor protection laws under SEBI, leaving many investors outside the ambit of protective regulations. Additionally, the decentralized and often cross-border operation of platforms impedes regulatory outreach and timely interventions. Current consumer protection frameworks in India drawn from the Consumer Protection Act, 2019 and financial sector legislations do not specifically address VDA-related disputes, contributing to gaps in effective grievance redressal. Consumer forums and civil courts face challenges in adjudicating disputes involving technology-dependent transactions, where digital evidence and blockchain records may require specialist knowledge. Many VDA investors, especially those unaware of due diligence procedures, resort to public interest litigation or human rights complaints, underscoring a systemic demand for institutionalized, accessible dispute resolution mechanisms within the VDA domain.

The ethical obligation of VDA service providers to ensure transparency, fair dealing, and informed consent is emerging as a critical area. While Indian regulations mandate Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance, there is limited legal enforcement of marketing standards or mandatory risk disclosures specific to VDAs. This regulatory lacuna raises concerns about consumer exploitation, particularly of vulnerable demographics drawn into high-risk, volatile asset classes with little investor education. Furthermore, the environmental impact of energy-intensive proof-of-work consensus mechanisms presents an ethical externality often overlooked in regulatory discourse, necessitating inclusion in holistic stakeholder protections.

Internationally, frameworks like the EU's MiCA regulation impose robust investor protection measures, including pre-issuance disclosure, advertising standards, custodial safeguards, and complaint handling processes, serving as potential models for India. Singapore's Payment Services Act also integrates risk-based licensing with ongoing supervisory reviews emphasizing consumer education and complaint management. Adopting tailored elements

[6] 15. 3rd Revision of Circular for Registration of Virtual Digital Asset Service Providers in FIU-IND as Reporting Entity, FIU-IND (Sept. 15, 2025), https://fiuindia.gov.in/pdfs/downloads/VDASP15092025.pdf.

from such frameworks, India can strengthen its consumer protection by enacting a dedicated VDA investor protection code, mandating standardized disclosures, KYC and AML enhancements, and a financial ombudsman scheme adapted to blockchain-enabled transactions.

Technological solutions also play a pivotal role in protection mechanisms. Smart contracts with integrated risk alerts, multi-signature wallets with embedded fraud-prevention protocols, decentralized identity identities facilitating transparent and consented data sharing, and blockchain analytics for real-time market surveillance are promising tools to enhance consumer trust and regulatory oversight. Encouraging adoption of privacy-enhancing technologies while ensuring regulatory transparency creates a balanced paradigm preserving investor rights without curtailing innovation.

In conclusion, India's emerging VDA regulatory architecture must prioritize comprehensive investor protection and ethical market conduct to sustain confidence and drive inclusive digital asset adoption. Legislative reforms need to define clear regulatory perimeters, institutionalize specialized dispute resolution, enforce transparency and risk disclosure, and integrate innovative technology tools. Only through an integrated legal and ethical framework can India build a resilient and mature VDA market that safeguards investors, promotes fair practices, and aligns with global standards of consumer protection.

15. CONCLUSION AND SUGGESTIONS

The study reveals that India's current legal framework for Virtual Digital Asset transactions is fragmented and reactive, adequately addressing tax and anti-money laundering obligations but lacking a cohesive, innovation-friendly approach to cybersecurity and data privacy. Major regulatory gaps remain in addressing blockchain-specific challenges such as transaction immutability, pseudonymity, and cross-border enforcement. The multiplicity of regulators without a unified oversight body creates overlaps, jurisdictional ambiguity, and compliance inefficiencies. Recommended reforms include enacting a comprehensive VDA-specific regulation that integrates cybersecurity, data protection, investor protection, and AML compliance. This statute should mandate privacy-by-design architectures, clear standards for wallet and exchange security, rapid incident reporting, and dispute resolution mechanisms tailored to the VDA ecosystem's unique features. Establishing a single regulatory authority or an empowered coordination forum would enhance consistency and regulatory certainty. Alignment with global standards such as MiCA and FATF should be pursued to facilitate international cooperation and investor confidence.

Looking forward, the roadmap for future-ready data protection in blockchain involves fostering innovation through regulatory sandboxes and encouraging adoption of cutting-edge privacy technologies like zero-knowledge proofs and decentralized identities. Public awareness campaigns and capacity-building for regulators are critical to keep pace with technological advances. Continuous monitoring of the evolving regulatory landscape globally will ensure that India's framework remains agile and supportive of both investor protection and technological growth.

16. RECOMMENDATIONS

In light of the analysis of India's existing legal and regulatory framework governing Virtual Digital Assets (VDAs), several targeted recommendations emerge to strengthen cybersecurity, data privacy, and investor protection while fostering innovation.

First, there is an urgent need for a ***comprehensive, VDA-specific legislative framework*** that integrates financial regulation, cybersecurity standards, data protection obligations, and consumer protection norms. Such a statute should clearly define VDAs, Virtual Asset Service Providers (VASPs), and decentralized finance (DeFi) activities, thereby reducing interpretational ambiguity and regulatory fragmentation.

Second, ***privacy-by-design and security-by-design principles*** must be statutorily mandated for VDA platforms. Regulatory standards should explicitly require robust key-management protocols, segregation of customer assets, secure wallet architectures (hot and cold wallets), periodic cybersecurity audits, and transparent breach-disclosure mechanisms tailored to the unique risks of blockchain-based systems.

Third, institutional reform is essential. Establishing a ***single nodal authority or an empowered inter-agency coordination mechanism*** for VDAs would enhance regulatory coherence among RBI, SEBI, MeitY/CERT-In, FIU-IND, and the Data Protection Board. Such coordination would streamline compliance, prevent regulatory arbitrage, and strengthen enforcement effectiveness.

Fourth, India should actively ***harmonize its regulatory approach with international best practices***, particularly the EU's MiCA Regulation and FATF guidelines, while adapting them to domestic socio-economic conditions. This would improve cross-border enforcement, facilitate international cooperation, and enhance investor confidence.

Finally, regulatory sandboxes and public-private partnerships should be expanded to encourage ***responsible innovation***, enabling regulators to better understand emerging technologies such as zero-knowledge proofs, decentralized identity systems, and privacy-preserving smart contracts before mainstream adoption.

17. LIMITATIONS OF THE STUDY

The present study is subject to certain limitations inherent in its scope and methodology. First, the research adopts a ***doctrinal and qualitative approach***, relying exclusively on secondary sources such as statutes, judicial decisions, policy documents, and scholarly literature. Consequently, the study does not incorporate empirical data, stakeholder interviews, or technical audits of VDA platforms, which could provide additional practical insights.

Second, the analysis is confined primarily to the ***Indian legal and regulatory framework***, with comparative references limited to selected jurisdictions such as the European Union and

Singapore. While these comparisons offer valuable perspectives, they do not represent an exhaustive global survey of VDA regulation.

Third, the ***rapidly evolving nature of blockchain technology and regulatory policy*** poses an inherent limitation. Legislative amendments, judicial pronouncements, and international regulatory developments may alter the relevance of certain observations over time.

Lastly, the study focuses predominantly on ***centralized VDA intermediaries***, while decentralized finance (DeFi) protocols and fully autonomous systems pose regulatory challenges that are still emerging and remain insufficiently addressed in current legal discourse.

18. SCOPE FOR FUTURE RESEARCH

The evolving Virtual Digital Asset ecosystem presents significant avenues for future scholarly inquiry. Future research may adopt ***empirical and interdisciplinary methodologies***, incorporating technical cybersecurity assessments, investor behavior studies, and regulatory impact analyses to complement doctrinal findings.

Further studies could examine the ***regulation of decentralized finance (DeFi)*** in greater depth, particularly issues of accountability, governance, and legal personhood in autonomous blockchain systems. Comparative research across a wider range of jurisdictions may also yield insights into regulatory convergence and divergence in global VDA governance. Another promising area for future research lies in exploring the ***compatibility of privacy-enhancing technologies***, such as zero-knowledge proofs, decentralized identity frameworks, and off-chain data architectures—with statutory data protection obligations under Indian law. Additionally, future studies could focus on ***consumer protection and dispute resolution mechanisms*** specific to VDAs, including the feasibility of specialized tribunals, arbitration frameworks, or ombudsman models for digital asset disputes. Finally, continuous research is needed to assess the ***long-term socio-economic and ethical implications*** of VDAs, including financial inclusion, environmental sustainability, and algorithmic governance, to ensure that regulatory responses remain balanced, adaptive, and future-ready.

CRYPTO CONSUMER PROTECTION IN INDIA: EVALUATING REGULATORY GAPS IN MISLEADING PROMOTIONS, EXCHANGE FAILURES, AND GLOBAL BEST PRACTICES

Karan Gupta
2nd Year Law Student B.A.L.L.B (Hons)
Christ (Deemd to be University) Bengaluru

Om Chopra
2nd Year Law Student B.A.L.L.B (Hons)
Christ (Deemd to be University) Bengaluru

Abstract

The rise of VDAs has taken hold faster than expected, creating a need for a new entity to cover their growing market share and usage. This has created a new group of investors who are interested in VDAs but are also exposed to many new/unknown risks, therefore creating a unique opportunity for significant retail investment in these digital products. The current regulatory structure in India for VDAs is highly fragmented and lacks a coherent approach to addressing key system deficiencies, including the misleading use of advertising and influencer promotion, the absence of transparency in exchange mechanisms, and the lack of a dedicated consumer protection framework. In addition to establishing taxation laws for VDAs and instituting AML obligations under the PMLA, 2002, India's intervention is also evident inthe enforcement of core consumer-facing risks. References to real-life failures of VDA companies, such as Vauld and GainBitcoin, indicate that for affected investors, there are limited options for recovery or remedy due to jurisdictional and administrative confusion between various regulatory entities, including the RBI, SEBI, FIU-IND, and MeitY. While theoretically, the CCPA (2019) provides a method of remedy for such consumers, there isa lack of clarity regarding decentralized platforms. Through a comparative analysis of the regulatory approaches adopted by the UK, Singapore, and the EU, the study examines India's regulatory challenges within an international framework, highlighting the need for consumer protection through solvency protections, custodial responsibilities, and an accessible grievance process. The study asserts that an Integrated VDA Consumer Protection Code should be developed for India, which includes regulations on market conduct, the separation of custody responsibilities, insurance protections, dispute resolution mechanisms, and initiatives to promote financial literacy, to provide adequate consumer protection in the evolving digital asset marketplace.

Key Words: Virtual digital assets, consumer protection framework, crypto-asset regulation, comparative regulatory models, investor protection mechanism

INTRODUCTION

The swift growth of Virtual Digital Assets (VDS), which encompasses cryptocurrencies, digital bonds, non-fungible tokens (NFTs), and other blockchain-based assets, has significantly changed the global exchange-based financial system. The rapid development of VDS was necessary to stabilize the international financial market after the 2008 financial crisis, which aimed to eliminate intermediaries such as banks and financial institutions, thereby changing the way we think about storing and transferring money. Virtual Digital Assets (VDS) are unique digital, identifiable files that generate vast economic benefits similar to traditional assets. However, they exist entirely in digital form, supported by blockchain cryptography for the security and identification of their users. This paradigm shift not only challenges financial institutions, such as banks, but also raises the very foundational question of regulatory challenges in governing these VDSs nationwide.[1]

The journey of India towards adopting Virtual Digital Assets (VDS) has been rooted in and inspired by the vision of digitalization, driven by the widespread adoption and expansion of UPI payments throughout the country. India, with a vast young and technology-driven population, supplemented by the rapid adoption of digitalization and increased use of Internet services, has led to the explosive growth of Virtual Digital Assets (VDS) in India. With the parallel development of digitalization, India has also witnessed a surge in crypto retail investors, a unique modern phenomenon that has fundamentally reshaped India's traditional financial system. Currently, India has one of the highest crypto adoption rates, with around 100 million users expected by 2025, surpassing the projected USD 6.4 billion mark. This was mainly due to the significant economic benefits derived from Virtual Digital Assets (VDS), as investors are attracted by high-return expectations, easy access, and the adoption of digitization, which has led to increased awareness of blockchain-based financial systems worldwide, especially in India.[2]

However, the very foundational feature that makes Virtual Digital Assets (VDA) attractive to retail investors is its unique decentralization and borderless transactions, which also make it highly susceptible to risk, particularly for retail investors who operate in a less regulated environment for Virtual Digital Assets (VDA). For long years, India's legal Landscape of VDA was unclear, neither officially banned nor controlled by a specific statute. Although the Income Tax Act has attempted to regulate VDA through Section 2(47A) of the act, and the further imposition of a 30% tax on VDA profits, along with 1% of TDS[3],demonstrates how India's legal landscape is trying to regulate it in response tothe need and necessity of this digital era. Initially, the regulations were introduced by the RBI with a warning against the use of VDA, which was followed by a blanket ban in 2018 through an RBI circular, referred

[1]CS (Dr.) Saibal Chandra Pal, *"Virtual Digital Assets under Direct Taxation"*, 55 Chartered Sec'y 66 (2025).
[2]Anjali Shukla, Prof. Dr. Monika Rastogi & Ms. Sweksha, *"The Evolution Of Digital Asset Regulation In India: Legal Implications, Economic Risks And Balancing Innovation With Consumer Protection"*, 13 Int'l J. Creative Rsch. Thoughts 362 (2025).
[3]Income-tax Act, No. 43 of 1961, Section 2(47) (India).

to as ***DBR.BP.BC.104/08/02/2017-18***[4]. This ban was subsequently struck down in a 2020 Supreme Court ruling in the Landmark case of ***Internet and Mobile Association of India vs. Reserve Bank of India, 2020***[5] ***and o***ne of the significant moments in the regulation of VDA occurred in the 2022 Union Budget, where, through an amendment to the Income Tax Act, 1961, it officially recognized VDA by introducing a stringent tax regime: a 30% tax on income transfer through VDA and a 1% deduction on transactions. Although the Indian Government's official introduction of VDA into the Indian financial economy is not consumer-friendly, as it aims to regulate money laundering and tax compliance, it overlooks the core issues of consumer protection and market integrity, which are closely intertwined.

LITERATURE REVIEW

1. Saibal Chandra Pal (2025) and Anjali Shukla et al. (2025): According to academic writings, India's Virtual Digital Asset system is characterized by a lack of regulatory clarity. Saibal Chandra Pal (2025) and Anjali Shukla et al. (2025) argue that a reactive mechanism regarding Virtual Digital Assets is more closely related to taxation and money monitoring than consumer protection. As there is no specific statutory system, it creates a situation of "legal indeterminacy," which denotes assets being acknowledged for taxation but lacking proper legal protection under statutory laws. Various research studies highlight that "the reliance on a pluralistic system of regulations scattered between RBI, SEBI, and FIU-IND has created an unorganized regulatory framework characterized by a lack of coherence in regulation" (Reddy, 2022). Although it can be stated that FIU-IND's strategies for preventing money laundering are adequate to some extent, they overlook retail investors, exchange insolvencies, and custodial failures. It has been observed that "the vulnerability of consumers may be further exacerbated due to the jurisdiction less, decentralized nature of VDAs, which allows their operators to function beyond jurisdiction to target Indian investors."

Under comparative analysis of jurisprudence, the Reserve Bank of India's reluctance to regulate is highly unusual in comparison to jurisdictions that recognize consumer protection as the foundation upon which the regulation of cryptocurrencies is established. Markets, in the view of Arner, Buckley, &Zetzsche (2023) themselves placed in the absence of standards related to either custody or solvency, left to rely entirely upon consumer risk is intrinsic to the current body of literatures with significant findings that might otherwise be described in the following manner: That consumer protection must proceed rather than follow the establishment of markets in the VDA industry finds highly informative support within the current body of literatures.[6]

[4]Reserve Bank of India, *"Prohibition on dealing in Virtual Currencies (VCs)"*, Circular No. RBI/2017-18/154, DBR.No. BP.BC.104/08.13.102/2017-18 (Apr. 6, 2018), https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2632

[5]Internet & Mobile Ass'n of India v. Reserve Bank of India, (2020) SCC OnLine SC 275 (India).

[6] Shukla, A., Rastogi, M., & Sweksha. (2025). *"The evolution of digital asset regulation in India: Legal implications, economic risks, and balancing innovation with consumer protection"*. International Journal of Creative Research Thoughts, 13(2), 362–372.https://www.ijcrt.org/papers/IJCRT2504287.pdf

2. Darmody and Zozulya (2023): Influencer-operated crypto-marketing has been identified recently in scholarly publications as a threat to consumer autonomy. The relationship between celebrity endorsements and distorted investment choice has been interpreted by scholars of behavioral finance based on Social Learning Theory and the Halo Effect. McLeod (2025); Perera (2023). Empirical investigations have established that when individuals of great popularity promote high-risk financial services, consumers tend to underestimate the risks and overestimate their legitimacy.

A critical analysis of the legal literature suggests that the over-reliance on self-regulation, as seen in the ASCI guidelines, is normatively correct; however, in practice, it lacks legal bite. According to researchers, the role of disclaimers, as important as they are, may not carry the same weightage as that of the influencer's testimonial in the case of a crypto ad, where the legitimacy of the influencer's credentials can potentially override the danger signals in the text, according to Darmody and Zozulya (2023), who add that misleading crypto ads are characterized not by the commission of direct falsities, but by the omission of key facts.

Comparative literature highlights the enforcement-focused models that exist in the contexts of the U.S. and the EU. Moreover, the fines imposed by the SEC on individuals such as Kim Kardashian and other so-called influencers have been recognized as an example that reflects the deterrent model for the internalization of misinformation costs (Zetzsche& Papakonstantinou, 2022). On the other hand, the absence of enforceable liability is recognized in Indian literature as enabling influencers to be driven by financial incentives rather than being concerned with the public's well-being.[7]

3. Sharma, S. (2023): Cases of exchange failures and crypto fraud have been recorded and documented within existing literature as a result of inadequately regulated digital assets. The documentation by Chainalysis (2022) and the Federal Trade Commission within the US shows that these cases of fraud within crypto result in financial losses that are inherent characteristics of these systems, which often operate without regulation and licensing. Concluding from these findings, it can be seen that certain studies carried out by research within India have identified additional events related to GainBitcoin and Vauld.It is recognised in legal interpretations of the Consumer Protection Act of 2019 that it is theoretically applicable to crypto disputes but has functional shortcomings (Sharma, 2023). According to consumer law experts, the CPA is characteristically responsive, remedying what is already lost, whereas crypto markets require a preemptive policy due to their inherent volatility and technological nature. Moreover, the decentralized nature of many of these crypto platforms makes it difficult to allocate responsibility, making the concept of "service deficiency" obsolete.

[7] Darmody, K., &Zozulya, O. (2023). *"Misleading crypto advertising and consumer harm: A comparative review"*. Computer Law & Security Review, 49, 105843. https://doi.org/10.1016/j.clsr.2023.105843 (last visited on December 23, 2025)

A comparative analysis of the EU MiCA regulation and Singapore's MAS framework highlights how specialized regulation of crypto-assets effectively combines consumer protection with oversight of finance, cybersecurity, and custodial liability (Paech, 2024). These approaches acknowledge that the main risks for investors are not confined to sales-related issues, but can also derive from operational issues, liquidity, or governance risks. Furthermore, in this regard, all works in this field have reached a consensus on a crucial observation: consumer protection laws cannot serve as a substitute for industry-specific regulation of cryptocurrencies. Authors of all works have recommended establishing a system of licensing, separating assets, disclosing information, and resolving disputes in cryptocurrencies in accordance with their nature.[8]

RESEARCH OBJECTIVES

The rapid growth of Virtual Digital Assets and the increase in consumer exposure to Financial, technological, and regulatory risks have heightened the need for an assessment of existing legal and regulatory regimes regarding their adequacy. Currently, there is no comprehensive Consumer-Centric Regulatory Mechanism in place; therefore, a deeper investigation into the various types of Investor Vulnerabilities, Enforcement Gaps, and Regulatory Comparisons will be required. Therefore, this study will focus on the following Research Objectives.

RO_1: The first is to find out what problems consumers will have when using Digital Assets from a legal, economic, and psychological perspective. To do this, it will look at how misleading promotions or failed exchanges may contribute to the consumer's perception of risk.

RO_2: Secondly, it will evaluate how effective the current Indian laws (such as the Consumer Protection Act and Self-Regulation Advertising Guidelines) are in protecting consumers against any harm caused by VDA activity.

RO_3: Thirdly, it will assess the regulatory measures implemented by other countries to protect VDA customers.

RO_4: Finally, it will suggest changes to laws and policies within India that would enhance consumer protection within the VDA ecosystem.

RESEARCH QUESTIONS

RQ_1: What impact do false advertising or promotions, advertisements from social media influencers, and poor risk assessment disclosure have on consumer behaviour regarding Virtual Digital Assets (VDAs) in India?

[8] Sharma, S. (2023). *"E-commerce and digital consumer protection in India: A critical study".* Criminal Law Journal, 1–12.

RQ_2: What are the specific regulatory and legal deficits within India's current regulatory laws concerning VDAs that subject consumers to financial and operational risks?

RQ_3: How effective are India's existing consumer protection laws, particularly the Consumer Protection Act 2019, in addressing grievances arising from misleading promotions and exchange failures in the Virtual Digital Assets (VDA) market?

RQ_4: What regulatory lessons can India draw from global frameworks such as the EU's MiCA, the UK's FCA guidelines, and Singapore's MAS model to develop a comprehensive and enforceable consumer protection regime for VDAs?

RESEARCH METHODOLOGY

The methodology of this research study uses doctrinal and analytical approaches to investigate. A thorough review of statutes, regulatory guidelines, judicial decisions, policy papers, and academic literature about Virtual Digital Assets and consumer protection in India is undertaken. The research also uses qualitative research methods, including content analysis and comparative legal analysis, to identify regulatory deficiencies in relation to false advertising, exchange failure, and investor protection mechanisms. Additionally, regulatory models from select international jurisdictions have been analyzed against a comparative framework to identify best practices applicable to India. All primary legal research has been performed using only publicly accessible data to maintain the integrity of the legal analysis and to support the accuracy, objectivity, and academic credibility of the findings.

REGULATORY VOID IN INDIA'S VDA ECOSYSTEM: NEED FOR A COMPREHENSIVE CONSUMER PROTECTION FRAMEWORK

The regulatory framework for virtual digital assets in India presents a significant challenge due to its monotonous nature and underdevelopment in existing laws. This leads to the existence of a grey area under which consumer risks are exacerbated. The first point of contention arises due to the absence of a specific law governing Virtual Digital Assets (VDAs), which may include trading, custody, redemption, and insolvency of these assets[9].While Section 2(47) formalizes these, they are only for taxation purposes. Furthermore, the division between the RBI and SEBI leads to **"regulatory pluralism without coherence,"** resulting in overlapping jurisdictions and uncertainty for both investors and service providers. BI has been skeptical about this area due to concerns over sovereignty and stability, leading to the adoption of restrictive measures, which means that the RBI does not informally promote investment VDAs.

On the other hand, the **Securities and Exchange Board of India (SEBI)** has refrained from claiming formal jurisdiction over VDAs.SEBI-regulated entities, such as mutual funds and Alternative Investment Funds (AIFs), are explicitly prohibited from exposure to cryptocurrency or crypto-derived products, indicating regulatory skepticism but without a

[9] Reserve Bank of India, *"Financial Stability Report"*86–89 (Dec. 2021), https://rbi.org.in/

corresponding supervisory framework. By contrast, the **Financial Intelligence Unit – India (FIU-IND)** has emerged as a de facto regulatory authority, but only for anti-money laundering (AML) and counter-terror financing (CFT) compliance. VDA service providers operating in India are required to register with FIU-IND under the Prevention of Money Laundering Act (PMLA), maintain transaction records, and report suspicious activities. However, this framework is narrowly confined to financial integrity concerns; it does not extend to consumer grievance redressal. Furthermore, the roles of the **Ministry of Electronics and Information Technology (MeitY) and the Ministry of Finance** also create a problem, as these ministries actively engage in decision-making processes and form legislative responses, but have not established a sector-specific authority for regulating VDAs.

A sector-specific grievance redressal mechanism is the need of the hour for regulating such assets. The absence of a dedicated financial regulator and a lack of statutory dispute resolution mechanisms to address sector-specific problems related to cryptocurrencies have led to the creation of bigger loopholes for the commission of crimes in this sector. The absence of a structured grievance-redressal mechanism is a critical weakness in India's VDA framework. With no dedicated financial regulator for crypto, investors lack a standardized forum to address issues such as withdrawal freezes, exchange shutdowns, hacks, or insolvency. Civil suits offer little relief, particularly when exchanges operate offshore, which creates jurisdictional and enforcement barriers. Policy analyses emphasize that consumer protection—not taxation or AML compliance—is the most urgent regulatory gap. Without precise redressal mechanisms, custody norms, or compensation mechanisms, retail investors remain vulnerable, undermining the confidence and long-term stability of the VDA ecosystem.

INFLUENCER-DRIVEN CRYPTO PROMOTION AND CONSUMER RISK: ANALYZING LIABILITY AND MISREPRESENTATION

The rapid transformation of VDA in India was accompanied by an aggressive marketing strategy aimed at promoting it through celebrities, social media influencers, and other channels to attract consumers and influence their investment choices and behavior in an unregulated crypto system, which is highly risky. Several well-established theories rightly point out why some celebrity and social media influencer endorsements are so powerful, particularly in shaping financial choices. Social Learning theory, also known as Bandura's theory, demonstrates how people are influenced by their role models or admired models they believe in. This theory posits that individuals acquire new behaviors not only through direct experience but also by observing others and witnessing the consequences of their admired actions.[10] This theory has direct implicationsfor the cryptography strategy. The companies intentionally choose celebrities and social media influencers for VDA's promotion, as most people follow those they admire, and as a consequence, create a market for crypto enhancement, even though it operates in an unregulated environment.

[10]Saul McLeod, *"Albert Bandura's Social Learning Theory"*, Simply Psychology (Oct. 16, 2025), https://www.simplypsychology.org/bandura.html

Furthermore, the Halo Effect theory is defined by its tendency for a person's positive traits, opinions, and expressions to influence how others judge unrelated attributes. For instance, if a celebrity is admired and popular, then this admiration is often transferred to the product they endorse. [11]This directly applies to VDS's promotional market, where an admired celebrity or social media influencer promoted highly risky VDAs. As a result, the consumer genuinely believes the promotional service or product was of high quality or had stable returns due to the promotion by a trustworthy person. This directly influences investor opinion, thinking, beliefs, and rational judgment about VDA, and it has such a significant impact that they often orchestrate internet risks in crypto promotions.

These theories clearly demonstrate why VDA promotions by celebrities and social media influencers have a disproportionate impact on investors' rational assessment of risk and returns when making investment decisions. When the endorsement was backed by biases that shape consumer behavior or rational assessment patterns, it became a significant problem, especially in India's crypto-unregulated market. To counterbalance the cognitive biases shaped by celebrity and social media influencers, ASCI has introduced mandatory guidelines while promoting VDA on platforms.

Thus, despite the ASCI's strict and mandatory guidelines, which were issued on 1st April 2022, requiring all VDAs, influencers, and advertisements to carry a disclaimer while advertising Particular ads for VDS, the mandatory disclaimer should read as follows:

Crypto Products and NFTs are unregulated and highly risky. There may be no regulatory recourse for any loss from such transactions."[12]

Despite such strict guidelines issued by ASCI in 2022 alone, it came to notice that over 400 crypto advertisements by social media influencers and celebrities had violated these mandatory disclaimer rules. In various instances, such as that of the famous YouTuber Lakshay Chaudhary, who has 3.05 million subscribers on YouTube, advertisements for cryptocurrency, specifically for CoinSwitch, were promoted without the mandatory disclosure requirement. Similarly, an Instagram Account named "*The Financial Yogi"* has over 41.8 K followers and promoted an advertisement of *"iForex Crypto"*in a video, which again omitted this mandatory requirement. Furthermore, the YouTube channel "*Money Tech," with* over 153,000 subscribers, shared a short video promoting "*Binance"* without mentioning the high risk associated with these Crypto Assets due to the lack of regulatory measures in India. In February 2025, ASCI published data on compliance with its guidelines,

[11] Ayesh Perera, *"Halo Effect In Psychology: Definition and Examples, Simply Psychology"*(Sept. 7, 2023), https://www.simplypsychology.org/halo-effect.html.

[12]Advertising Standards Council of India (ASCI), *"Guidelines for Virtual Digital Assets and Linked Services*", Section 1.1 (Feb. 23, 2022), https://www.ascionline.in/wp-content/uploads/2022/09/vda-guidelines-press-release-feb-23.pdf

which shows that over 69% of India's top social media influencers and celebrities failed to display a mandatory disclaimer.[13]

According to Rohit Aggarwal, Co-Founder & CEO of Alpha Zegus, one of the significant reasons for omission of this ASCI mandatory guidelines of showing disclaimer while promoting any advertisement of Crypto Assets was that companies and brands intentionally omit this because they firmly believe that showing a disclaimer will reduce the active engagement and will definitely skip the commercial aspect of this video.
Further, Shudeep Majumdar, Co-Founder of Zefmo Media, argues that the mere attraction of "*Lure of Money",* which is combined with weak or even a lack of regulation of Crypto Assets, together combine to force the ASCI to take strict action, which is further exemplified by non-compliance with mandatory guidelines of ASCI showing disclaimer before advertising any Crypto Assets promotion video. For instance, micro-influencers with 10K-50K Followers are charging between $20K-$50 per crypto advertisement, while top Celebrities charge over $ 1.5 million per advertisement.[14]

Thus, the core problem lies between the lack of regulatory power of ASCI guidelines and the immense influence of advertisements, which is also associated with financial interests. Even though ASCI guidelines were detailed, they were only self-regulatory, as seen in social media influencers and celebrities often prioritizing commercial interests over audience or consumer safety to whom they are addressing.

One of the prime and recent examples of High Risk associated with crypto advertising without showing a disclaimer is WazirX, a crypto asset. In July 2024, a significant cybersecurity breach occurred, where it was estimated that Hackers had stolen over $230 million worth of Ethereum-based tokens.This is one of the classic examples of how operational risk is extremely very high in crypto yet still many social media influncers and celebrity choose to promote these ads for their commercial interest rather than consumer interest even if they decide to promote, the central point is that the lack of a disclaimer was one of the significant reasons why everyday consumers were exploited through these advertisements. [15]While the platform promotescryptocurrency advertisements based on Brand or Company Interest by labeling them as modern and exciting opportunities, it simultaneously omits a disclaimer regarding custodial failures, frequent hacks, or wallet breaches, which puts the consumer or audience at risk of exploitation.

However, internationally, this has precisely the opposite effect due to the strict enforcement of guidelines and penalties for their violations. In 2022, the U.S. Securities and Exchange Commission (SEC) fined Kim Kardashian USD 1.26 million for promoting a crypto

[13] Imran Fazal, *"Influencers Push Crypto Ads in Rampant Violation of ASCI Guidelines"*, Storyboard18 (Dec. 3, 2024), https://www.storyboard18.com/brand-marketing/influencers-push-crypto-ads-in-rampant-violation-of-asci-guidelines-49176.htm
[14]Id.
[15] Press Trust of India, *"WazirX accused of running persistent disinformation campaign by Liminal while users wait for court updates,"* The Hindu (India), Oct. 7, 2024, https://www.thehindu.com/sci-tech/technology/wazirx-accused-of-running-persistent-disinformation-campaign-by-liminal-while-users-wait-for-court-updates/article68786444.ece

advertisement for EMAX on her Instagram Account without disclosing that she was paid for this promotion. This demonstrated how, at the International level, even though breaches occurred, it was backed by sanctions and penalties, showing that "Paid Promotion" by celebrities and social media influencers is subject to security laws that threaten the consumer interest at large.[16]

Further, former NBA Player Paul Pierce was penalized and punished for the EtherumMax promotion controversy. The U.S. Securities and Exchange Commission (SEC) found that he was paid to promote EMAX tokens worth more than USD 244,000 and also used misleading advertisements. For instance, he shared a screenshot showing a significant profit from EMAX, which was deceptive, as his own holdings were low.[17]

Similarly, in a high-profile case, the SEC charged several celebrities, including Lindsay Lohan, Jake Paul, Ne-Yo, Akon, and others, for promoting Tronix (TRX) and BitTorrent (BTT). According to regulatory filings, the celebrities' paid tweets contributed to the creation of misleading market sentiment regarding TRX/BTT's legitimacy and growth potential.[18]

This case highlights how influencers and public figures can mislead consumers by promoting cryptocurrency without providing adequate transparency regarding compensation or the speculative nature of the assets.

CRYPTO-RELATED FRAUDS AND EXCHANGE INSOLVENCIES: STRUCTURAL VULNERABILITIES IN THE INDIAN VDA MARKET

The rapid expansion of crypto assets in India was accompanied by the unprecedented rise in scams, fraud, and excessive failures of these crypto assets on their platform, leaving investors in an uncertain market. Unlike the traditional market or financial system, the crypto platform operates in a hostile market environment, which allows it to exploit investors through deceptive practices and promotions due to significant gaps in enforcement resulting from a lack of specific laws or regulations governing its enforcement. Even at the global level, this scam is one of the biggest concerns, as the US Federal Trade Commission notes that consumers or investors have lost approximately USD 1 billion in crypto scams and frauds between 2021 and 2023, primarily due to promotions and advertising by celebrities or social media influencers.[19]

---

[16] U.S. Sec. & Exch. Comm'n, Press Release: *"SEC Charges Kim Kardashian for Unlawfully Touting Crypto Security"*(Oct. 3, 2022), https://www.sec.gov/newsroom/press-releases/2022-183

[17] AP News, *"Pierce to Pay $1.4M to Settle With SEC on Crypto Violations"*(Feb. 17, 2023), https://apnews.com/article/29911f62a5cf02e2ea1d6249b9a8ccdd).

[18] Jessica Wang, *"Lindsay Lohan, Jake Paul, and Ne-Yo Among Celebs in Crypto Violation Complaint, Entertainment Weekly"*(Mar. 22, 2023), https://ew.com/celebrity/lindsay-lohan-jake-paul-ne-yo-celebrities-crypto-violation-complaint/.

[19] *"Reported Crypto Scam Losses in 2021 Top $1 Billion, Says FTC Data Spotlight, Fed. Trade Comm'n"* (June 22, 2022), https://www.ftc.gov/business-guidance/blog/2022/06/reported-crypto-scam-losses-2021-top-1-billion-says-ftc-data-spotlight.

One of the major types of crypto scams is the Rug Pull, where developers or managers of the crypto platform suddenly disappear after raising money from users or investors, commonly seen in scam tokens such as fake DeFi Projects. In 2021, Rug Pull alone accounted for nearly USD 2.8 billion of stolen crypto money by the legitimate investors[20]

Another widespread scam and fraud involved the extensive expansion and exploitation of trading apps, which are designed to facilitate financial transactions. In reality, these apps steal investors' funds at large and are one of the largest types of scams in today's era, especially in Asia, including India.[21]These types of scams and frauds are not merely isolated,x but they are routine, leading to a catastrophic, uncertain environment for the investors

One of the classic examples where a crypto exchange poses a high risk due to exchange failure is the Singapore-based crypto platform Vauld. These platforms are entrusted with users' assets, but suddenly freeze or halt withdrawals of their users' assets. In July 2022, this Singapore-based crypto platform suddenly halted withdrawals and suspended exchanges, citing market stress.[22]Thishighlights how fragile a curated environment, such as a platform,is when it works in an unregulated environment, especially in a country like India. Initially, it presents itself as one of the most promising, safe, and high-yielding investment options, offering interest returns between 12% and 40% annually, which is intended to create a positive impression in the minds of consumers, suggesting stability with high returns. It's not only one side,it has another side as well. CNBC reports that Vauld has suffered a loss of approximately USD 200 million due to the crypto market crash. It failed to maintain sufficient liquidity or assets to honor customer withdrawals.[23] The model on which Vaukd was founded was high-risk, involving the rehypothecation of customers' or consumers' assets, with no robust or reserve structure in place when these assets went into insolvency.

Furthermore, it also highlights the significant and restrictive role of jurisdiction-having governed by, as well as having its headquarters in Singapore, which is governed by the local insolvency laws of that country. At the same time, the majority of the affected customers reside in other countries, especially India, which is the most severely affected. This cross-

[20]Chainalysis Team, *"Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity"*,Chainalysis (Jan. 6, 2022), https://www.chainalysis.com/blog/2022-crypto-crime-report-introduction/

[21]*"Hyderabad Police Sounds Alert Over Alarming Rise of Online Trading, Investment Scams"*, Deccan Chronicle (Telangana), Oct. 30, 2025, https://www.deccanchronicle.com/southern-states/telangana/hyderabad-police-sounds-alert-over-alarming-rise-of-online-trading-investment-scams-1913630

[22]Press Trust of India, *"Singapore-Based Crypto Platform Vauld Freezes Trades"*, The Hindu (July 4, 2022), https://www.thehindu.com/sci-tech/technology/singapore-based-crypto-platform-vauld-freezes-trades/article65602269.ece.

[23]CNBC – Vauld Halts WithdrawalsSophie Mellor, *"Crypto Lender Vauld Halts Withdrawals as Market Crash Takes Its Toll"*, CNBC (July 4, 2022), https://www.cnbc.com/2022/07/04/crypto-lender-vauld-halts-withdrawals-as-market-crash-takes-its-toll-.html

border crypto transaction support, enabled by the unregulated crypto environment, further aggravated consumer or customer grievances.[24]

GainBitcoin was another one of the largest Crypto Ponzi schemes in India, affecting customers or consumers across multiple districts of the Country. It was launched in 2015 by Amit Bhardwain, who intended to attract investors by promising an interest rate of 10%. Monthly return for 18 months guaranteed. The GainBitcoin scam operates as an MLM-style pyramid scheme, encouraging initial investors who receive payouts to fund new investors, in turn recruiting new people. As more people joined these schemes, the perception of joining was influenced by factors such as peer pressure, family pressure, social media promotion, and celebrity endorsements. In 2023, the CBI launched raids in several states, across 60 locations, seizing laptops and wallets containing ₹2,394 Crore. However, the most striking implication is that despite the raids. According to the CBI, most investors did not recover their invested money due to the issue of complex traceability, as most of their assets were converted into foreign wallets, which was further exacerbated by the lack of a protected, regulated environment in India.[25]

Another prominent example was BitConnect, the world's largest Ponzi scheme, and India was one of the countries most heavily affected by the crypto platform. It positioned itself by promising 1% guaranteed daily high return, which is even mathematically impossible for any legitimate investment. The promoters, especially the most influential, were Carlos Matos, who utilized viral videos and emotional seminars to expand their reach. In a very short span of time, it was heavily expanded to various states in India, especially Maharashtra, Gujarat, and Punjab. However, it was starkly different from the traditional Ponzi scheme as it used a token-based system. Investors are encouraged to purchase BitConnect Coin (BCC), which must be locked on the platform to earn a guaranteed interest rate of 1%. However, in reality, no such system exists initially. When global regulatory agencies such as the U.S. SEC began to investigate, it suddenly and abruptly shut down. In January 2018, more than 90% of tokens experienced a significant decline in value. More than 10,000 entire portfolio investors saw their entire portfolios vanish on this platform in a very short period of time. Even though several complaints against IRs were filed, due tothe lack of a regulatory environment in India regarding VDA and the transfer of these investors' funds into foreign or international wallets, it became impossible to investigate them.

However, beyond financial losses to the investor, the rise of these crypto platforms also gives rise to violent crimes, which are directly linked to crypto fraud. For example, a man was kidnapped and tortured for several days because the kidnappers believed that the man possessed Bitcoins worth lakhs. Further, a brutal case where people tortured a man from Kerala for many days because his associate believed he held massive Bitcoins, an amount of

[24]Pawan Nahar, "*A Look at What Went Wrong With Vauld"*, Economic Times (July 7, 2022), https://economictimes.indiatimes.com/markets/cryptocurrency/where-did-vauld-go-wrong-and-what-led-it-to-the-verge-of-end
ngame/articleshow/92728479.cms](https://economictimes.indiatimes.com/markets/cryptocurrency/where-did-vauld-go-wrong-and-what-led-it-to-the-verge-of-end-game/articleshow/92728479.cms).

[25]*"CBI Conducts Searches at 60 Locations in Rs. 6,600 Crore GainBitcoin Cryptocurrency Scam Under Supreme Court Directive"*,TaxTMI (Feb. 25, 2025), https://www.taxtmi.com/news?id=35256.

approximately USD 485 Crores, and he was tied to a chair for two days continuously and forced to reveal the wallet password. [26]It is not a single isolated case, another case where a businessman was abducted and, in exchange for his return, demanded a ransom of 200 BTC, which is a massive amount then, which shows how digital currency becomes another or an alternative mode of demanding ransom. Further in Gujarat, a group of rogue police officers was kidnapped by business people and extorted around 200 BTC from him, worth more than 13 crore at that time, which, later, in August, 2025 Court sentenced 14 people, including an IPS Officer and a BJP MLA, to life imprisonment for playing an active role in extorting BTC from business people[27].

EVALUATING THE CONSUMER PROTECTION ACT, 2019, IN THE CONTEXT OF VIRTUAL DIGITAL ASSETS

The Consumer Protection Act, 2019 (CPA), represents a significant shift in India's consumer law framework, particularly in its efforts to address digital markets, online transactions, and platform-based service delivery. As Virtual Digital Assets (VDAs) have rushed from niche instruments to mainstream investment products, the central question that arises is whether existing consumer legislation—particularly the CPA—can protect VDA buyers in cases of fraud, exchange failures, misleading advertisements, or deficiencies in exchange services. While the Act undoubtedly offers certain conceptual avenues for relief, it also reveals substantial structural and practical [28]limitations when applied to an asset class as decentralized, volatile, and technologically complex as cryptocurrencies.[29]

To begin with, the foundational question is whether a VDA investor qualifies as a "consumer" under the Act. The CPA defines a consumer as a person who buys goods or avails services for a consideration. When an individual uses a centralized crypto exchange to purchase digital tokens, pay trading fees, or utilize platform-based services, the relationship fits within this definition. The exchange is offering a paid service—whether it is facilitating transactions, maintaining wallets, or providing access to trading infrastructure—and therefore can be seen as a service provider. On this basis, a VDA investor should be able to approach consumer commissions for disputes involving blocked withdrawals, system outages, non-execution of trades, or misleading descriptions of services. This theoretical recognition is often sufficient [30]to file complaints, and several investors have attempted to do so.

---

[26] Kalyan Das, *"Man Killed After Being Tortured for Days Over Bitcoins"*, Hindustan Times (Aug. 31, 2019), https://www.hindustantimes.com/india-news/man-killed-after-being-tortured-for-days-over-bitcoins/story-A18ipLTQCrlFphgBPYHxoI.html

[27] Gaurav Doshi, *"Ahmedabad Court Sentences 14 in Bitcoin Extortion and Kidnapping Case"*, India Today (Aug. 29, 2025), https://www.indiatoday.in/india/law-news/story/ahmedabad-court-sentences-14-in-bitcoin-extortion-kidnapping-case-2778775-2025-08-29

[28] Jaideep Reddy, *"Regulating Virtual Currencies in India: Considerations in Balancing Innovation and Consumer Protection"*, 15 Indian J. L. & Tech. 110 (2022).

[29] S. Sharma, *"E-Commerce & Digital Consumer Protection in India: A Critical Study"*, Criminal L.J. (2023).

[30] Cyril Amarchand Mangaldas, *"Global Crypto Developments: Lessons for India's Regulatory Regime"*(FIG Paper No. 40, 2025).

However, the challenge begins when one examines the nature of the "service" being offered and the unique structure of VDA markets. Crypto exchanges do not simply provide a digital interface; they engage in complex custodial, technological, and financial operations. Many exchanges are incorporated outside India, maintain servers abroad, or rely on decentralised technical infrastructures. The absence of clear regulatory recognition of VDAs as goods or financial products further complicates their classification. While the CPA does not require an item to be legally recognized as currency or a security to be considered a "product," the uncertainty surrounding the legal character of VDAs makes adjudicating such matters much more difficult for consumer courts.

The CPA's provisions on deficiency of service appear highly relevant in theory. If an exchange abruptly suspends withdrawals, delays transactions without reason, suffers a preventable security lapse, or mismanages user funds, these could all amount to deficiencies. Likewise, misleading advertisements, exaggerated claims of returns, and downplaying of risks could constitute unfair trade practices. The crypto sector in India has witnessed aggressive promotional campaigns, especially during market booms, with celebrity endorsements and influencer-driven marketing that often obscure the speculative and high-risk nature of the asset class. In such instances, the CPA provides consumers with a conceptual basis to challenge misinformation or deceptive conduct.[31]

Another limitation stems from the decentralized nature of many VDA services. Decentralized exchanges (DEXs), peer-to-peer protocols, and self-custody wallet providers do not operate like traditional service providers with a clear managerial entity. Their operations are governed by code, not by contractual promises. Applying CPA's notions of responsibility, deficiency, or fault becomes challenging when no identifiable company controls the platform or when a distributed network of nodes executes the service's functions. The CPA, designed for clear provider-consumer relationships, struggles to address systems where the "service" is automated, anonymous, or open-source.

Even in cases involving Indian or India-facing exchanges, the CPA lacks specialized provisions needed to regulate a high-risk and technologically sophisticated domain like crypto. The Act does not mandate financial audits, proof-of-reserve disclosures, cybersecurity standards, custody norms, or [32]risk-warning requirements specific to VDA platforms. Traditional consumer law frameworks assume a relatively predictable relationship between providers and consumers. In contrast, VDA markets are characterized by technological vulnerabilities, liquidity risks, high volatility, and exposure to global markets. Without domain-specific rules, the CPA operates as a reactive mechanism—available only after harm occurs—rather than a preventive regulatory shield that could reduce the likelihood of damage in the first place.

Moreover, unlike in sectors such as banking, insurance, or securities, there is no specialised regulator to supplement the CPA with technical scrutiny or sector-specific oversight. In the absence of such coordination, consumer fora are often ill-equipped to interpret complex

[31] Tech Observer, *"India's Crypto Market Faces Regulatory Gaps as Investor Risks Mount"*(2024).
[32] Business Standard, *"Crypto Advertising and the Problem of Misleading Claims in India"*(2023).

blockchain-related evidence, evaluate the security architecture of exchanges, or assess liability in cases involving smart contract vulnerabilities. The result is that the CPA, while legally applicable, lacks the operational capacity to deliver justice in most crypto-related disputes.

The broader issue is conceptual rather than merely procedural: VDAs involve a level of risk that cannot be adequately managed solely through general consumer law. Investors often face losses due not only to misconduct by service providers but also because of market volatility, cyberattacks, technical failures, and global regulatory developments. A consumer protection framework must therefore move beyond issues of service deficiency to address structural safeguards, such as mandatory insurance, custodial standards, independent audits, and real-time transparency norms.

In essence, the Consumer Protection Act, 2019, provides only a limited and imperfect remedy for VDA consumers. While it can be invoked for clear cases of misrepresentation or platform failure, it cannot substitute the need for a specialised, crypto-centric regulatory framework. What the Indian VDA ecosystem requires is a dedicated set of rules addressing the unique nature of digital assets, combining consumer law, financial regulation, cyber law, and cross-border enforcement. Until such a framework emerges, the CPA will continue to offer symbolic protection rather than substantive relief for India's rapidly growing population of digital asset investors.[33]

COMPARATIVE EVALUATION OF GLOBAL VDA REGULATORY FRAMEWORKS: LESSONS FOR INDIA

The rapid expansion of virtual digital assets across global financial markets has exposed a persistent structural injustice: the lack of a uniform, reliable, and enforceable consumer-protection standard for retail investors. While there are examples, including the United Kingdom, Singapore, and the European Union, that have established sophisticated statutory and supervisory frameworks to regulate promotions, custody, licensing, and operational integrity, many emerging economies remain within regulatory grey zones defined by fragmented oversight and asymmetric risk allocation. This fragmented landscape puts retail participants, who are often financially unsophisticated, at a disproportionately high risk of misinformation, mis-selling, asset loss, and systemic vulnerabilities. The injustice is not derived merely from market volatility but from gaps in regulation that fail to impose accountability on service providers and leave consumers to fend for themselves in a technologically complex and opaque domain bereft of meaningful safeguards. Here, a comparative regulatory analysis is crucial for highlighting existing inequities and informing the development of robust investor-protection regimes.

1. United Kingdom's Regulatory Approach: Strengthening Crypto Market Conduct And Consumer Safety

[33] Economic Times, *"Crypto Withdrawals Frozen: Indian Investors Left Without Legal Recourse"*(2022).

When we examine the existing parallel legislation in the United Kingdom and Singapore, we encounter significant loopholes related to retail protections. In the UK, the FCA's 2023-2024 financial promotion rules place heavy emphasis on ensuring that consumers fully understand the risks before investing: first-time buyers must be granted a mandatory 24-hour cooling-off period after viewing a direct offer promotion, and firms are prohibited from offering "refer a friend" bonuses or other incentives that may induce impulsive investing. Furthermore, it mandates all markets to be fair, avoiding fraud and scams. It also ensures that the investor has the necessary experience and categorizes them into different risk segments,such as sophisticated and high-net-worth individuals. The Payment Services Act (PSA) requires digital payment token (DPT) service providers to obtain licenses, maintain strict client-asset segregation, manage technology and cyber risks, and comply with AML/CFT obligations. In contrast, Singapore's regulatory regime under MAS is broader and more structural, concentrating less on how crypto is sold and more on who can legitimately offer it and how such firms must operate. Crucially, MAS discourages widespread retail involvement not only by disclosing information but also by severely restricting public marketing. To avoid trivializing the serious risks involved, providers are only permitted to advertise tokens on their own corporate websites or official mobile applications. They are also prohibited from using social media influencers, placing ATMs for cryptocurrency services in public areas, or advertising in public spaces. In contrast to the FCA's model, which permits more open access but imposes "friction" and warning mechanisms, the MAS's model establishes substantive gatekeeping: firms must be licensed, advertising is strictly regulated, and incentives such as referral bonuses or free tokens are prohibited, particularly for retail users. The public is further shielded from the systemic risks of speculative finance by Singapore's increasing restrictions on high-risk activities,such as lending and token staking. A. Singapore treats cryptocurrency more like a regulated financial service, requiring strict prudential controls over the firms themselves—their capital, technology, and [34]operational behavior—rather than merely restricting how these firms can communicate with the public. In contrast, the UK's scheme effectively treats crypto promotion as a "high-risk product" and regulates its communication.[35]

By bringing cryptocurrency and digital assets completely under the purview of the Financial Services and Markets Act (FSMA), the UK is moving toward a comprehensive, statute-level regulatory framework. Activities such as custody, trading, stablecoin issuance, and platform operations will soon require full FCA authorization, similar to how traditional financial services are regulated, thanks to several FCA consultation papers and the proposed Crypto Assets Order 2025. Prudential stability, operational resilience, and governance are prioritized in the UK. Businesses must adhere to the Senior Managers & Certification Regime, maintain robust [36]internal controls, segregate client assets under the CASS framework, and meet capital and liquidity standards. Additionally, consumer protection is a top priority, particularly in limiting deceptive advertising, tightening regulations on financial promotions, and investigating restrictions on credit-based cryptocurrency purchases. The upcoming

[34] Adrian Ang & Alexander Fong, *"Digital Tokens and Customer Protections, Part 1 (on Singapore DPT regulation under the PSA)*", Bits & Bytes (TRAIL, NUS Law) (Oct. 30, 2023).
[35]Id
[36] HM Treasury, *"Future Financial Services Regulatory Regime for Cryptoassets: Response to the Cryptoasset Consultation"* (Oct. 2023)

Crypto asset Reporting Framework (CARF), which will require thorough transaction reporting for tax compliance, is another way the UK is incorporating cryptocurrency into larger international transparency initiatives. The UK's approach, which aims to mitigate the risks associated with volatile and frequently opaque VDA markets while establishing a mature, institution-ready ecosystem, is generally more legislative and supervision-intensive.

2. Singapore's Mas-Led Regulatory Model: A Structured Approach to VDA Consumer Protection

On the other hand, the regulatory framework for virtual digital assets is overseen by the Monetary Authority of Singapore, which has a well-structured and consumer-focused approach. This regulation is anchored in the Payment Services Act and the MAS, which is backed by high security technological standards and measures to prevent conflicts between different entities. It also [37]provides a channel for mandatorily disclosing and clearly listing policies related to virtual digital assets. Furthermore, regulations enforcing a ban on unlicensed platforms like Binance.comare also in place, making the platform more consumer-friendly. Furthermore, this mandatory licensing also serves as a filter,eliminating the risks of unnecessary scams and reducing other risksassociated withthe diversion of funds through alternative channels,such as terror financing via investment in virtual assets. This approach highlights Singapore's commitment to creating a safer environment and a level playing field.

3. The Eu Mica Framework: A Comprehensive Model For VDA Licensing And Consumer Protection

The world's first comprehensive, codified legal framework, created expressly to regulate crypto-assets, service providers, and market behavior throughout a sizable, multi-jurisdictional economic bloc, is the European Union's Markets in Crypto-Assets Regulation (MiCA). MiCA, which was passed in 2023 and will take effect gradually from 2024 to 2025, specifically addresses the issues that nations like India are still facing, including advertising discipline, consumer protection, systemic risk mitigation, custody safeguards, and licensing clarity[38]. As academics point out, MiCA was born out of the realization that disparate national strategies among EU members were compromising market integrity and permitting regulatory arbitrage, necessitating a single model for both investor security and innovation.

The risk-tiered licensing framework at the heart of MiCArequires all Crypto-Asset Service Providers (CASPs) to obtain authorization from national regulators in accordance with harmonized EU-wide standards. These include minimum capital requirements, executive fitness assessments, audit obligations, and stringent organisational controls. The gap in India, where exchanges operate without uniform consumer-facing duties or statutory solvency requirements, is directly addressed by this licensing regime. The custody provisions of MiCA are especially noteworthy: According to recent legal analyses supporting greater custodial

[37] Marina E. A. Frediani, *"Crafting the Future of Finance: A Comparative Analysis of Cryptocurrency Regulation in the Global Economy"*, 13 J. Fin. Risk Mgmt. 193 (2024).
[38] Dirk A. Zetzsche& Vagelis Papakonstantinou, *"Regulating Crypto-Assets: The EU's Markets in Crypto-Assets (MiCA) Framework"*, 33 Eur. Bus. L. Rev. 1121 (2022)

accountability, CASPs are responsible for "loss of crypto-assets resulting from operational failures," must segregate client assets, and have strong cybersecurity measures in place.

Another hallmark of MiCA is its explicit consumer-protection architecture. Issuers of stablecoins [39](referred to as "asset-referenced tokens") must publish detailed whitepapers, disclose risks, and maintain reserve assets. Restrictions on deceptive promotions, transparent fee disclosures, and mandatory risk warnings all reflect broader concerns expressed in comparative studies looking at the adverse effects of crypto-ads across jurisdictions. These requirements contrast with India's permissive advertising environment, where influencers and exchanges have [40]historically promoted VDAs without enforceable disclosure obligations.

Crucially, MiCA also requires CASPs to set up easily accessible and prompt dispute-resolution procedures by introducing a structured complaint-handling and redressal mechanism. According to academics, this represents a significant step toward institutionalizing investor rights in [41]cryptocurrency markets, a gap that has been consistently highlighted in studies of emerging digital-asset economies. All things considered, MiCAdemonstrates how thorough and uniform regulation can promote innovation while protecting consumers. In terms of licensing, custody, disclosure, advertising standards, and grievance procedures in particular, it provides India with an example of accountability and clarity. Stable regulatory environments not only mitigate consumer [42]harm but also improve long-term market credibility, as research consistently demonstrates.[43]

BRIDGING INDIA'S VDA REGULATORY GAPS: POLICY IMPERATIVES AND FUTURE DIRECTIONS

The examination of these ten sections reveals that systemic consumer risks, regulatory ambiguity, and structural vulnerabilities characterize India's rapidly growing VDA ecosystem, all of which cannot be addressed by piecemeal policy solutions. There is a regulatory void where exchanges operate without clear accountability, investor dispute resolution remains inadequate, and consumers are frequently exposed to platform collapses, deceptive advertising, and sophisticated frauds due to the lack of a dedicated, coherent legal framework and conflicting institutional positions between the RBI, SEBI, and MeitY. Although the E-commerce Rules and the Consumer Protection Act, 2019 provide theoretical remedies, their applicability is restricted by jurisdictional limitations, the absence of obligations specific to cryptocurrencies, and the particular difficulties presented by decentralized digital assets. Cybersecurity flaws, SIM swap incidents, and inadequate data

[39] Kathleen Darmody & Olena Zozulya, *"Misleading Crypto Advertising and Consumer Harm: A Comparative Review"*, 49 Comput. L. & Sec. Rev. 105843 (2023)
[40] Douglas W. Arner, Ross P. Buckley & Dirk A. Zetzsche, *"Crypto-Assets, Financial Stability, and the Evolution of Global Regulation"*, 38 J. Int'l Banking L. & Reg. 512 (2023).
[41] European Commission, *"Regulation (EU) 2023/1114 of the European Parliament and of the Council on Markets in Crypto-Assets (MiCA)"*, Official Journal of the European Union (2023).
[42] European Securities and Markets Authority (ESMA), "*Technical Standards on Crypto-Asset Service Providers Under MiCA"*(2023).
[43] Philipp Paech, *"The Future of EU Digital Finance Regulation"*,MiCA as a Harmonising Instrument, 45 Eur. L. J. 233 (2024)

protection procedures simultaneously increase operational risks. A comparative review of global frameworks—including EU MiCA's licensing and custody safeguards, the UK FCA's stringent advertising controls, and Singapore's MAS-driven risk-mitigation model—highlights that robust consumer protection is achievable only when regulation is precise, centralised, and backed by enforceable market-conduct rules. Collectively, the findings underscore the urgent need for a unified VDA Consumer Protection Code, mandating licensing, solvency norms, insurance or escrow safeguards, transparent disclosures, and a specialized grievance redressal authority capable of addressing both centralized and decentralized market harms. Equally essential is an ecosystem-wide push for financial literacy to counter unrealistic expectations and reduce susceptibility to scams. As India continues to tax VDAs and witnesses growing retail participation, the policy imperative is unmistakable: safeguarding consumers is not merely a regulatory obligation but a prerequisite for building a trustworthy digital-asset economy, ensuring market stability, and enabling responsible innovation. Future research should explore optimal institutional design, insurance models, and cross-border regulatory interoperability to guide India's transition toward a mature, consumer-centric VDA regime.