FINANCIAL CYBER CRIME IN THE EMERGING WEB3 ECOSYSTEM: EVALUATING THE ADEQUACY OF INDIA'S CYBER LAW FRAMEWORK

[1]Meera PM
[1]Law and Legal Studies
[1]SASTRA UNIVERSITY

***Abstract*—Web3 technologies have evolved the structure of financial crimes. Financial cybercrime is now taking the shape of a category of crimes based on disintermediation, pseudonymity and cross-border movement with the support of cryptocurrencies, non-custodial wallets, decentralised exchanges, smart contracts, non-fungible tokens, and decentralised autonomous organisations. "This paper seeks to answer this question in respect of the Indian Cyber law. It looks at the Information Technology Act 2000, Bharatiya Nyaya Sanhita 2023, Prevention of Money Laundering Act 2002, Bharatiya Sakshya Adhiniyam 2023 and Bharatiya Nagarik Suraksha Sanhita 2023 and questions if they are sufficient to prevent, investigate, prosecute and remedy financial crime committed using Web3.**

It has taken a doctrinal approach, with comparisons drawn to the Markets in Crypto-Assets Regulation of the European Union and Payment Services Act of Singapore, and drawn on the guidelines of the Financial Action Task Force. The relevant Web3 crimes are aligned to the existing legislation to see the extent of existing law's reach, such as wallet compromising, phishing, rug pulls, smart contract exploits, ransomware, and layered money laundering.

A combination of technology agnostic offences and a perimeter not yet defined for AML make India's framework workable with several legal gaps yet to be addressed. No legislation exists today explicitly related to virtual assets, and the jurisdiction and legal responsibility are not well defined. Laws are also not explicit about the existence of decentralised and autonomous code-based actors. Further, international cooperation and legal frameworks for the tracing and recovery of digital assets are still underdeveloped, which makes it difficult to do. These gaps have a real-time sense of urgency because the National Cyber Crime Reporting Portal data indicate that the financial fraud losses reported have increased significantly in 2022–2024.

The paper conclude that India's current legal framework can respond to harm after it occurs, but it does not yet fully regulate the virtual asset ecosystem that can create such risks. This paper therefore suggests introducing a dedicated law for virtual digital assets, strengthening specialised agencies to investigate cyber-financial crimes, improving international cooperation in line with FATF Recommendation 15, and learning from the regulatory approaches followed by the European Union and Singapore.

***Index Terms*—Web3, financial cybercrime, virtual digital assets, Information Technology Act 2000, Prevention of Money Laundering Act, Bharatiya Nyaya Sanhita, FATF, comparative cyber law**

I. INTRODUCTION

1.1 Background of the Study

The term "Web3" is increasingly used to describe a new phase of the internet built around decentralised

technologies. Digital financial activities are increasingly being conducted through distributed ledger technology (DLT), reducing reliance on traditional centralised intermediaries such as banks and other financial institutions. Blockchain technology allows value to be recorded, transferred and even programmed without a trusted third party standing as intermediary[1]. Decentralisation is one of the biggest strengths of Web3, but it also presents major regulatory challenges as it can be hard to determine who is responsible, what rules it falls under and who is liable for it. The transactions can be decentralised without any intermediaries such as banks and are therefore more difficult to monitor. Criminals are able to exploit crypto wallets and blockchain systems and cross-border transfers are challenging to trace and recover funds. In fact, Europol has highlighted the fact that illicit funds now go through a series of new, lightly-regulated entities instead of one accessible entity[2], the Financial Action Task Force ("FATF") has also pointed to the "industrialisation" of virtual asset fraud by organised groups [3].

India's approach to virtual currencies has changed over time. It has included attempts to restrict them, court decisions that changed those restrictions, and gradual regulation through tax and anti-money-laundering laws. However, India still does not have one specific law that comprehensively regulates Web3 or virtual assets." The Reserve Bank of India's 2018 circular, which restricted banking services to cryptocurrency businesses, was struck down by the Supreme Court in *Internet and Mobile Association of India v. Reserve Bank of India* on grounds of proportionality[4]. After that judgment, the field was left to general statutes ie., the Information Technology Act 2000 ("IT Act"), the Indian Penal Code, which is now enacted as the Bharatiya Nyaya Sanhita 2023 ("BNS"), and the Prevention of Money Laundering Act 2002 ("PMLA"), which was extended to virtual digital asset ("VDA") service providers only in March 2023,

[1] "Nat'l Law Sch. of India Univ., Web3: A Tech and Policy Brief for India 3–5 (2023)."
[2] "Europol, Cryptocurrencies: Tracing the Evolution of Criminal Finances 6–8 (2022)."
[3] "FATF, Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs 2 (July 16, 2026)."
[4] "Internet & Mobile Ass'n of India v. Reserve Bank of India, 2020 SCC OnLine SC 275

through a Ministry of Finance notification[5]. "The BNS, the Bharatiya Sakshya Adhiniyam ("BSA") and the Bharatiya Nagarik Suraksha Sanhita ("BNSS") together reshape the procedural and evidentiary ground on which Web3 offences must now be investigated and proved. This paper examines whether India's existing laws can effectively address the unique features of Web3, including anonymous or pseudonymous transactions, the absence of intermediaries, permanent blockchain records, automated smart contracts, and the easy movement of digital assets across countries.

1.2 Statement of the Problem

India's criminal laws were designed particularly for traditional financial transactions that involve

banks, companies and identifiable physical locations. As web3 functions differently , it causes legal difficulties and uncertainty. The four major problems are:

1. Legal uncertainty as it is not sure whether the existing laws extend to criminal offences such as rug pulls or smart contract attacks.
2. Jurisdictional uncertainty as blockchain transactions are borderless and involves people all over the world and hence it is difficult to identify which laws to be applied. 3. Evidential uncertainty as authorities and courts find difficulty in analysing how to authenticate blockchain records, wallet information and digital transaction history as evidence against the financial crimes.
4. Regulatory uncertainty as it is ambiguous about which authority should be taken primary responsibility for virtual assets as RBI, SEBI, FIU-IND has separate roles and currently India does not have an exclusive virtual asset regulatory holder.

1.3 Aim and Objectives

This paper sets out to evaluate whether India's existing cyber and financial crime framework is adequate to the task Web3 poses, and to recommend reform where it falls short. The paper primarily identifies the parts of web3 which are most vulnerable to crime and the major types of financial cybercrime involving cyber web3. It examines whether India's existing laws such as IT Act, BNS,BNSS,BSA,PMLA are sufficient to deal with the financial cyber

[5] "Notification No. S.O. 1072(E), Ministry of Finance, Department of Revenue (Mar. 7, 2023) (India), issued under PMLA § 2(1)(sa)(vi)."

crimes.By examining Indian case law, regulatory measures, EU and Singapore practices, and FATF standards, the paper identifies the existing legal gaps and suggests reforms suited to India's legal and institutional system.

1.4 Scope and Limitations

The paper compares India with two jurisdictions which are EU and Singapore as EU relies on a comprehensive legal framework where Singapore focuses on a license based approach. The paper limits the comparison to two countries alone to provide a meaningful in-depth analysis rather than shallow or ambiguous analysis." The datas in the paper are not collected after conducting interviews or field research but based on official statistics and regulatory sources and hence the findings would be intricate rather than exhaustive

1.5 Research Questions

1. To what extent India's existing laws can be applied to specific financial web3 crimes? 2. Whether

there exists any gaps in existing Indian laws regarding web3 financial crimes?

3. What legal and regulatory changes could India introduce to address these gaps, while taking useful lessons from the EU, Singapore and FATF standards and ensuring that the proposed reforms are practical for India's existing legal and institutional system?

II. MAIN BODY

2.1 The Web3 Ecosystem: Conceptual Foundations

Web3 is a decentralised form of the internet that uses technologies such as blockchain, cryptocurrencies and smart contracts to allow users to interact and conduct transactions without relying entirely on traditional intermediaries such as banks or large technology platforms.A blockchain is a digital record of transactions that is shared and maintained by many computers network instead of one central authority. "Cryptocurrency is controlled through a private key, which is stored or managed using a digital wallet. In a custodial wallet, the exchange or service keeps control of the key, while in a non-custodial wallet, the user controls it themselves. This difference is important in criminal cases because it affects how authorities can trace, access, freeze, or recover the digital assets. A custodial exchange can be compelled to freeze or disclose assets; a non-custodial wallet generally cannot[6]. Centralised exchanges perform the fiat-to-crypto conversion function that banks once performed alone, which is why they are now the point at which most anti-money-laundering obligations attach, as "reporting entities" under the PMLA[7]. DeFi allows people to lend, borrow, and trade digital assets using smart contracts instead of banks or other intermediaries.NFTs are unique digital assets. They can also be used in investment scams and fake trading activities.DAOs are organisations that run through blockchain-based rules and community decisions. It can be difficult to decide who is legally responsible when something goes wrong.The common feature of these systems is that they do not depend on a central intermediary. Instead, they rely on automated code and users who may remain anonymous or pseudonymous, making regulation and criminal enforcement more difficult.

2.2 Typology of Financial Cybercrime in the Web3 Ecosystem

Based on crime patterns identified by Europol, Chainalysis, and Indian enforcement , this paper identifies eight common types of financial cybercrime involving Web3.

[6] "Nat'l Law Sch. of India Univ., Web3: A Tech and Policy Brief for India 7–9 (2023)."
[7] Notification No. S.O. 1072(E), Ministry of Finance, Department of Revenue (Mar. 7, 2023)

Crypto theft and wallet attacks involve the unauthorised transfer of assets from an exchange or wallet, usually achieved by compromising private keys through malware, social engineering or insider access.

Phishing and credential fraud Criminals use fake messages or wallet websites to trick people into giving away their private keys or approving fraudulent transactions.

Smart contract exploits take advantage of coding vulnerabilities, re-entrancy bugs, flawed access controls, oracle manipulation, to drain a DeFi protocol.

A rug pull happens when developers collect money from investors and then suddenly take the money or abandon the project.

Ransomware locks victim's files and documents in computer and demands payment in cryptocurrency as ransom in order to unlock the files.

Investment and Ponzi-type scams tricks people into investing in large sum promising high returns.

Crypto-based money laundering for moving illegal money through cryptocurrencies to conceal the sources before converting this to regular currency

NFT fraud involves using fake information or fake trading to mislead people about the value of NFTs.

2.3 Research Methodology

This study adopts a doctrinal research methodology, supported by comparative and policy analysis. It examines primary legal sources, including the IT Act, BNS, PMLA, BSA, BNSS and Income Tax Act, along with relevant rules, guidelines and Supreme Court decisions. Secondary sources include academic research, reports from RBI, SEBI, FATF and Europol, and blockchain industry reports. The study also compares India's framework with the regulatory approaches of the European Union and Singapore

2.4 Existing Indian Legal Framework

2.4.1 The Information Technology Act, 2000

The IT Act is the main law for computer-related offences in India, but it was created before Web3 and blockchain technology and its existing provisions are now being used to address some Web3-related crimes. Section 43 creates civil liability for unauthorised access to a computer resource[8], and section 43A imposes compensation liability on a body corporate that fails to secure sensitive personal data, which matters directly for exchange breaches[9]. Sections 66 to 66F build on this: section 66 criminalises the dishonest acts already covered by section 43[10], section 66C targets identity theft through fraudulent use of a password or

signature[11], section 66D covers cheating by personation[12], and section 66F reaches cyberterrorism[13]. Section 70B designates CERT-In as the national nodal agency for incident response[14], while section 75 extends the Act to offences involving a computer resource located in India, though this is of limited practical use against a blockchain that recognises no borders at all[15]. Sections 43 and 66 are easily mapped onto web3 wallet and exchange hacking, section 66C is the key/seed phrase extraction and section 66D is for phishing. At best, 66F could cover what would be at best a cyberterrorism attack on a systemically destabilizing DeFi exploit – but no one has actually tried to use 66F in court.

2.4.2 The Bharatiya Nyaya Sanhita, 2023

The BNS replaced the Indian Penal Code from 1 July 2024 and retains cheating under section 318, punishable by up to three years or five where the offender occupied a position of trust[16], alongside criminal breach of trust under section 316, punishable by up to five years or ten if aggravated[17]. Both provisions apply readily to investment scams and rug pulls. Section 111 of the BNS specifically creates an offence for organised crime, which is significant because organised criminal activity can involve coordinated and repeated illegal activities.

[8] "Information Technology Act, No. 21 of 2000, § 43, INDIA CODE (2000)."
[9] "Id. § 43A."
[10] "Id. § 66."
[11] "Id. § 66C."
[12] "Id. § 66D."
[13] "Id. § 66F."
[14] "Id. § 70B."
[15] "Id. § 75."
[16] "Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, § 318, INDIA CODE."
[17] "Id. § 316."

Its definition of "economic offence" extends to cybercrime, breach of trust, forgery and mass-marketing fraud carried out by a syndicate, and it carries punishment up to life imprisonment along with a mandatory fine[18]. This provision could be useful for large rug pull scams carried out by organised groups. However, terms such as "economic offence" and "cybercrime" are broad, so it is still unclear how courts will apply them and creates uncertainty for accused persons.

2.4.3 The Prevention of Money Laundering Act, 2002

The PMLA criminalises the process or projection of proceeds of crime as untainted property[19], and it requires the businesses to verify the identity of customers and report to the authorities if anything has been found suspicious. The development that actually matters for Web3 is the Ministry of Finance's notification of 7 March 2023, which brought five categories of VDA activity within the definition of designated business or profession: exchange between VDA and fiat, exchange between forms of VDA, transfer,

safekeeping or administration of VDA, and participation in an issuer's offer and sale of VDA[20]. Entities carrying out these activities, including offshore VDA service providers with Indian users, must now register with FIU-IND under the AML/CFT Guidelines issued on 10 March 2023[21].

2.4.4 The Bharatiya Sakshya Adhiniyam, 2023

The BSA replaced the Indian Evidence Act on 1 July 2024. It is important in Web3 cases because blockchain records, wallet details, transaction records and digital communications are all forms of electronic evidence. The admissibility of a record shall not be denied on the basis that it is an electronic record pursuant to section 63[22]. The new section 63 replaces the previous section 65B and will accept computer output as evidence without the production of the computer, but still requires dual certification from the device operator and expert[23]. The Supreme Court's jurisprudence on the predecessor provision remains the governing law here. In Anvar P.V. v. P.K.

[18] "Id. § 111(1). See generally A.Z.B. & Partners, Overview of the Bharatiya Nyaya Sanhita, 2023 (Jan. 2024)." [19] "Prevention of Money Laundering Act, No. 15 of 2003, § 3, INDIA CODE (2002)."
[20] "Notification No. S.O. 1072(E), Ministry of Finance, Department of Revenue (Mar. 7, 2023) (India)." [21] "Fin. Intelligence Unit-India, AML/CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (Mar. 10, 2023)."
[22] "Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, § 61, INDIA CODE."
[23] "Id. § 63; see also Bhatt & Joshi Assocs., Electronic Evidence Under BSA 2023: Section 63 Certificate Requirements & Supreme Court Interpretation (2025)."

Basheer the Court held that certification is mandatory[24], and it clarified in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal that this requirement is a sine qua non, though the certificate can be procured with court assistance where necessary[25]. These decisions will shape how blockchain and wallet evidence gets proved under section 63 going forward. The more permissive approach once taken in State (NCT of Delhi) v. Navjot Sandhu no longer represents the law[26].

2.4.5 The Bharatiya Nagarik Suraksha Sanhita, 2023

The BNSS replaced the Code of Criminal Procedure 1973 and governs search, seizure and freezing procedure[27].The law does not provide specific procedures for seizing private keys or freezing crypto assets held in smart contracts. Investigators have to use the existing power of search, seizure and PMLA. This is challenging as digital assets do not have a physical address and can be transferred in a matter of seconds.

The Finance Act 2022 amended Section 115BBH of the Income Tax Act 1961, introduces a special tax regime for VDA transfer income with no loss set-off and requires a tax deduction at source[28].It is a tax measure, not a criminal law, but it creates records of VDA transactions that can help investigators trace financial activities

2.5 Regulatory Framework

2.5.1 The Reserve Bank of India

The RBI's posture toward virtual currencies was set by its April 2018 circular, which directed regulated entities to stop providing banking services to cryptocurrency businesses[29]. The Supreme Court struck that circular down in Internet and Mobile Association of India for failing the proportionality standard under Article 19(1)(g); the Court found no demonstrated harm and no evidence that less intrusive alternatives had even been considered[30]. It is worth being precise about what the Court actually decided. The court held that the way by which RBI used its power

[24] "Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India)."
[25] "Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India)." [26] "State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 S.C.C. 600 (India), overruled on this point by Anvar P.V., (2014) 10 S.C.C. 473."
[27] "Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, INDIA CODE."
[28] "Income-tax Act, No. 43 of 1961, § 115BBH, INDIA CODE (as inserted by Finance Act, 2022)." [29] "Reserve Bank of India, Circular No. DBR.No.BP.BC.104/08.13.102/2017-18 (Apr. 6, 2018) (India)." [30] "Internet & Mobile Ass'n of India v. Reserve Bank of India, 2020 SCC OnLine SC 275 (India)."

in this case is not valid, but did not remove RBI's power to regulate virtual currencies. RBI does not have separate licensing system for VDA exchanges. RBI's reports generally discuss digital payment fraud and cybersecurity as part of wider digital risks rather than treating virtual assets as a separate category.

2.5.2 The Securities and Exchange Board of India

SEBI becomes a relevant authority when web3 involves investment or security schemes. India does not define whether such digital assets are payments or investments. This creates uncertainty about the regulatory authority that should deal with web3.

2.5.3 The Financial Intelligence Unit-India

FIU-IND is now the principal financial intelligence node for Web3-related laundering. It receives suspicious transaction reports from registered VDA providers and passes actionable intelligence to the Enforcement Directorate, but its effectiveness depends entirely on how many providers actually register. Reports suggest that only a small number of these businesses registered after the March 2023 notification. Foreign crypto platforms that serve Indian users are also required to register, but many still remain outside the Indian regulatory system.

2.5.4 CERT-In and Cybersecurity Governance

The CERT-In Directions of 28 April 2022, issued under section 70B(6) of the IT Act, require service providers and body corporates, a category that includes Indian VDA exchanges, to report cybersecurity incidents within six hours, synchronise system clocks and retain logs for 180 days within India[31]. These requirements can help investigators look into security breaches at crypto exchanges. However, their scope is limited because non-custodial wallets and decentralised protocols are not considered "bodies corporate"

under the Directions and therefore fall outside these requirements.

2.6 Application of Existing Law to Specific Web3 Crimes

Table 1 links the eight types of Web3 financial crime with the relevant Indian laws and briefly explains how effectively those laws apply to each type of crime.

[31] "CERT-In, Directions Under Section 70B(6) of the Information Technology Act, 2000 (Apr. 28, 2022) (India)." Page 14 of 27

Web3 Crime Typology	Primary Statutory Provision(s)	Supporting Provision(s)	Doctrinal Fit
Crypto theft / wallet attacks	IT Act sec.43, 66	BNS sec. 305 (theft, if property analogy applies)	Good — unauthorised access is clearly captured
Phishing / credential fraud	IT Act sec. 66D; BNS sec.318 (cheating)	IT Act sec. 66C (identity theft)	Good — personation and cheating provisions apply directly
Smart-contract exploits	IT Act sec. 43(b), (i) (unauthorised access/ introduction of contaminant)	BNS sec. 111 (organised crime, if syndicate-run)	Weak — code-level causation and attribution untested
Rug pulls	BNS sec. 316, 318 (breach of trust, cheating)	PMLA sec. 3 (if proceeds laundered)	Moderate — depends on locating and identifying developers
Ransomware	IT Act sec. 43, 66; BNS sec. 111 (cyberterrorism/ organised crime, if applicable)	IT Act sec. 66F (cyberterrorism, extreme cases)	Good on liability; weak on cross-border attribution
Investment / Ponzi scams	BNS sec. 318, 111	SEBI regulations (if security-like token)	Good — well-settled cheating jurisprudence applies
Crypto-based laundering	PMLA sec. 3, read with Mar. 2023	FIU-IND AML/CFT Guidelines, 2023	Moderate — depends on VASP

	Notification		registration and cross-border cooperation
NFT-enabled fraud	BNS sec. 318 (cheating)	IT Act sec. 66	Weak — valuation and wash-trading concepts not addressed

Table 1: Mapping of Web3 Financial Cybercrime Typologies to Applicable Indian Statutory Provisions

2.7 Legal Gaps

Absence of a dedicated virtual asset statute : India regulates virtual digital assets through tax rules , anti money laundering rules and existing criminal laws. Unlike EU , India does not have comprehensive law which specifically deals with VDA that provides definition , regulatory authority and licensing requirements.The 2019 Cryptocurrency Bill was never passed, so India's VDA framework has developed gradually through notifications and existing laws rather than through a dedicated statute.

Jurisdiction : Section 75 of the IT Act extends the statute's reach to offences involving a computer resource located in India, but a blockchain simply has no fixed territorial home.

However, blockchain transactions are difficult to link to one country because the offender, victim, exchange and network participants may all be located in different countries. International legal procedures can also be too slow, as crypto assets can be transferred almost instantly and are difficult to recover once moved.

Anonymity and pseudonymity : Public blockchain are more transparent than cash dealings because all transactions are permanently recorded but the difficulty faced is to identify the person behind the wallet.This is easier when an exchange has KYC information, but much harder when crypto is transferred directly between two non-custodial wallets.

Smart contracts and code-based liability. Indian law has not worked out how liability should attach when harm is caused by code executing autonomously rather than by a discrete human act at the moment of harm. The literature on smart contract enforceability under Indian contract law has flagged this same gap[32].

Decentralised actors and DAOs. Neither the BNS nor the Companies Act treats a DAO as a legal person. That leaves prosecutors chasing individual, often pseudonymous, token-holders or developers instead of the collective entity whose governance decision actually caused the harm.

Asset recovery. The BNSS's search-and-seizure powers and the PMLA's attachment provisions were both designed for tangible or bank-held property , and neither offers a summary procedure for freezing

assets locked in an immutable smart contract or sitting in a non-custodial wallet. Once funds leave a compliant exchange, victim restitution becomes largely aspirational.

2.8 Enforcement Challenges

In addition to these legal gaps, four practical challenges also make enforcement difficult.

Tracing transactions across chain-hops and mixers requires specialist blockchain-forensic capacity that is unevenly distributed across Indian agencies, notwithstanding the availability of tools of the kind used by Chainalysis and TRM Labs[33]. **Cross-border investigation** depends on

[32] "Smart contracts and blockchain: legal issues and implications for Indian contract law, INT'L REV. L. COMPUTERS & TECH. (Taylor & Francis, forthcoming)."
[33] "Chainalysis, 2024 Crypto Crime Report 9–11 (2024)."

mutual legal assistance mechanisms that were never designed for the speed at which blockchain moves; FATF's Seventh Targeted Update identifies persistent gaps in licensing and international cooperation as the result[34]. Freezing or seizing crypto is relatively easier when it is held by an exchange because the exchange controls the assets. However, it becomes much more difficult with non-custodial wallets, where the user alone controls the private key and the law does not clearly explain how authorities can obtain it. Identifying the person behind a wallet address can also be challenging, especially when investigators have to rely on exchange KYC records or detailed blockchain analysis. The problem becomes even greater when foreign crypto platforms that are not registered in India are involved**.**

The official data shows that cybercrime in India has increased significantly. However, the data does not show how many of these cases involved virtual digital assets (VDAs), so it cannot be used to measure Web3 crime directly. It does, however, show that India's existing cybercrime system is already under increasing pressure

2.9 Comparative and International Perspective

2.9.1 FATF Standards

FATF extended Recommendation 15 to virtual assets and VASPs some years ago, and its 2021 guidance sets out a risk-based approach built around VASP licensing, due diligence, and the travel rule for originator and beneficiary information[35]. FATF says that although crypto regulation has improved, monitoring foreign crypto platforms and personal wallets remains difficult, which also makes criminal investigations harder.India's September 2024 Mutual Evaluation placed the country in the regular follow-up category, FATF's highest tier, while still flagging the need to expedite fraud prosecutions[36]. Overall, India's AML system follows international standards, but it is still unclear how effectively it works for Web3 and virtual assets because its practical use in this area has been limited.

[34] "FATF, Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs 3–5 (July 16, 2026)."
[35] "FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers 14–22 (Oct. 2021)."
[36] "FATF, Anti-Money Laundering and Counter-Terrorist Financing Measures — India, Mutual Evaluation Report 3, 47–52 (Sept. 2024)."

2.9.2 The European Union: Markets in Crypto-Assets Regulation

The EU's Markets in Crypto-Assets Regulation, fully applicable since 30 December 2024, offers the clearest comparative counterpoint to India's approach[37]. It harmonises definitions across the Union, requires authorisation of crypto-asset service providers with EU-wide passporting, and imposes governance, capital and cybersecurity requirements on them[38]. Where India relies on a fragmented, notification-based approach, the EU has a single statutory code that addresses licensing and consumer protection before harm occurs rather than after.

2.9.3 Singapore: the Payment Services Act 2019

Singapore takes a third path, regulating cryptocurrency as digital payment tokens under the Payment Services Act 2019, which requires a Monetary Authority of Singapore licence and compliance with AML/CFT obligations under Notice PSN02[39]. Amendments made in 2024 extended coverage to custodial services and cross-border transfers, closing loopholes of exactly the kind that persist in India's narrower, PMLA-only perimeter[40]. Singapore's licensing-based approach could provide India with a practical model for regulating virtual assets without the high cost and complexity of the EU's MiCA framework.

2.10 Findings

It is to be analysed from the comparison that India's existing criminal laws can deal with traditional crimes such as theft, cheating and money laundering but becomes weak when dealing with web3 crimes such as smart contract attacks, DAO related problems and NFT fraud. The BNS, BNSS, and BSA have strengthened investigation and prosecution mechanisms for organised crimes and electronic evidence but still lacks in completely addressing cross border jurisdiction and crimes using computer codes." India mainly relies on Anti Money Laundering rules than a comprehensive VDA licensing system. As compared to EU and Singapore, India lacks supervision and strong regulation for consumer protection. The reported financial fraud is

[37] "Regulation 2023/1114, of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, 2023 O.J. (L 150) 40."
[38] "Id. arts. 59–64, 85; see also Chainlink Labs, What is MiCA? EU's Markets in Crypto-Assets Regulation Explained (2025)."
[39] "Payment Services Act 2019 (Act No. 2 of 2019) (Sing.); Monetary Auth. of Sing., Notice PSN02: Prevention of Money Laundering and Countering the Financing of Terrorism — Digital Payment Token Service (2019)." [40] "Monetary Auth. of Sing., Regulation & Policy: Amendments to the Payment Services

Act (Apr. 2, 2024).”

increasing as compared to past years its high time that the system need to deal with new and developing crimes.

III. CONCLUSION

The study examined whether India’s existing cyber and financial crime laws are sufficient to deal with financial crimes arising from the web3 ecosystem. “The analysis shows that these laws can cover many web3 related crimes specifically similar to traditional offences such as fraud, theft and money laundering but these laws are not specifically designed for the unique features of web3.

India’s existing laws can deal with some Web3 crimes, but they do not cover everything. India has no specific VDA law, so rules on licensing, supervision and consumer protection are still unclear. Web3 transactions can also be difficult to trace because they may involve anonymous users and different countries. Crimes such as smart contract attacks, rug pulls and DAO-related fraud are difficult to deal with under traditional laws. Another challenge for freezing or seizing crypto is that the rules are primarily in place for real estate or bank accounts.

There are two reasons why these issues are important. In March 2023, India enacted the anti-money-laundering regulations to cover VDA (Virtual Data Address) service providers and the number of financial frauds reported rose significantly from 2023 to 2024. This demonstrates that India is moving towards further strengthening of its VDA system, albeit not in a law or via specific rules and notifications. While overall, the AML regime in India conforms to the FATF standards, the effectiveness of India's AML regime to address the newer variants of Web3 crime remains uncertain.

The study finds that while cyber laws in India can help punish a large number of crimes committed in the web3 space, the legal framework has not been specifically crafted for the Web3 space. The main gaps are the lack of clear rules for intermediaries, uncertainty about jurisdiction, and limited tools for investigating blockchain-related crimes.

IV. SUGGESTIONS FOR A PROPOSED REGULATORY REFORM

4.1 Enact a Dedicated Virtual Digital Asset Statute

The paper suggests that India should create one specific law for virtual digital assets (VDAs) which could clearly explain what VDAs and VASPs are and decide which authority will regulate them.It also suggests that crypto exchanges and custodians should follow rules on management, financial strength and customer protection. India could follow a simpler licensing system similar to Singapore.

4.2 Establish a Specialised Cyber-Financial-Crime Investigative Architecture

It recommends that the government must enhance the capability of the existing cybercrime units by equipping them with cybercrime experts in blockchain-forensics and suitable tools to tackle blockchain related crimes in India. These teams should closely collaborate with the Indian Cyber Crime Coordination Centre and avail the tools for blockchain analysis. Investigators and prosecutors also need to be trained on collecting and submitting blockchain and wallet records as evidence in accordance with Section 63 of the BSA.

4.3 Strengthen Cross-Border Cooperation Mechanisms

India needs to establish more expeditious cooperation processes between countries to investigate cryptocurrencies. It would enable Indian authorities to trace and recover crypto assets in Indian and other countries in a hassle free manner. India also needs to share information with countries wherein big online platforms are functioning and needs to collaborate more with international organisations like Europol and FATF.

4.4 Close the Offshore VASP Compliance Gap

Foreign virtual data stores (VDA) providers (FVPs) serving Indian users must be registered with FIU-IND and abide by Indian rules. If they do not register, alternative measures like limiting access for Indian users and payment systems should be taken. That way the registration requirement would be taken seriously rather than being a "paper tiger".

4.5 Develop a Procedure for Freezing Non-Custodial and Smart-Contract Assets

Clear rules governing how private keys, crypto assets can be addressed by authorities during investigations should be in place to support the BNSS and PMLA. These rules should ensure the accused's right to not incriminate himself or herself, and also delineate the circumstances under which disclosure of key evidence may be demanded. They should also provide an explanation on how assets identified on the blockchain can be frozen by the courts even if they are not held by a custodial wallet.

4.6 Clarify Regulatory Jurisdiction Between RBI, SEBI and FIU-IND

The responsibilities of the various regulatory bodies need to be clearly demarcated between RBI, SEBI and FIU-IND in India. The RBI could be responsible for payment related virtual assets, SEBI could be responsible for assets that act as securities/investments and FIU-IND could be responsible for anti-money-laundering requirements. It would be easier to avoid regulatory gaps with clearer responsibilities and nigh on impossible for dubious investment schemes to exploit the lack of clarity.

4.7 Improve Crime-Specific Data Collection

While capturing cybercrime data, it is important to note NCRB and Indian Cyber Crime Coordination Centre separately whether the crime involved a VDA or not (whenever it can be identified). Currently, there is no readily available data in this format. More data would enable law enforcement to get a clearer understanding of the magnitude of Web3 related crimes and further research on this subject area.

4.8 Directions for Future Research

The future research should be done on the actual scenario of the cases arising under PMLA and IT Act on VDA related cases, when the sufficient number of cases are available. It should also research the legal restrictions on the ability of an accused party to be compelled to provide a private key." Future research is also required to evaluate the impact of new FATF guidance and future legislation for Indian VDA on addressing the gaps in law and enforcement issues highlighted in this paper.

References

A. Statutes and Delegated Legislation (India)

[1] Information Technology Act, No. 21 of 2000, INDIA CODE.

[2] Prevention of Money Laundering Act, No. 15 of 2003, INDIA CODE (2002).

[3] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, INDIA CODE.

[4] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, INDIA CODE.

[5] Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023, INDIA CODE.

[6] Income-tax Act, No. 43 of 1961, § 115BBH, INDIA CODE (as inserted by Finance Act, 2022). Notification No. S.O. 1072(E), Ministry of Finance, Department of Revenue (Mar. 7, 2023) (India).

[7] Financial Intelligence Unit-India, AML/CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (Mar. 10, 2023).

[8] Reserve Bank of India, Circular No. DBR.No.BP.BC.104/08.13.102/2017-18 (Apr. 6, 2018) (India).

[9] Indian Computer Emergency Response Team, Directions Under Section 70B(6) of the Information Technology Act, 2000 (Apr. 28, 2022) (India).

B. Cases

[10] Internet & Mobile Ass'n of India v. Reserve Bank of India, 2020 SCC OnLine SC 275 (India). Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).

[11] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1

(India). State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 S.C.C. 600 (India).

C. Foreign and International Legal Instruments

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

[13] Payment Services Act 2019 (Act No. 2 of 2019) (Sing.).

[14] Monetary Authority of Singapore, Notice PSN02: Prevention of Money Laundering and Countering the Financing of Terrorism — Digital Payment Token Service (2019).

[15] Monetary Authority of Singapore, Regulation & Policy: Amendments to the Payment Services Act (Apr. 2, 2024).

D. Reports of International Organisations

[16] FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Oct. 2021).

[17] FATF, Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (July 16, 2026).

[18] FATF, Anti-Money Laundering and Counter-Terrorist Financing Measures — India, Mutual Evaluation Report (Sept. 2024).

[19] Europol, Cryptocurrencies: Tracing the Evolution of Criminal Finances (2022).

E. Industry Reports (Non-Legal Authority)

[20] Chainalysis, 2024 Crypto Crime Report (2024).

[21] TRM Labs, Crypto Crime Report (2024).

F. Academic Articles and Journal Commentary

[22] Sweta Panda & Amruta Das, Crimes on Cryptocurrency and Jurisdictional Challenges of Enforceability in India, INT'L J.L. MGMT. & HUMAN. (2026).

[23] Rudra Vashishth & Nancy Sharma, Cryptocurrency and Money Laundering in India: A Study Under the PMLA 2002, INDIAN J. LEGAL REV. (2026).

[24] Avadhesh Pratap Singh, Regulation of Virtual Digital Assets: The Journey, Challenges, and Way Forward, INT'L J.L. MGMT. & HUMAN. (2024).

[25] D. Suganthini & M.G., Guidelines on Legal Framework for Cryptocurrency in India, INT'L J.L. SCI. & INNOVATION (2024).

[26] Smart Contracts and Blockchain: Legal Issues and Implications for Indian Contract Law, INT'L REV. L. COMPUTERS & TECH. (Taylor & Francis).

[27] Muffliha Sadaf & T. Vaishali, Crypto Crimes: Legal Challenges and Regulation of Cryptocurrency in India (2023).

[28] Nat'l Law Sch. of India Univ., Web3: A Tech and Policy Brief for India (2023).

G. Professional and Government Commentary

[29] Trilegal, PMLA Framework on Virtual Digital Assets: Two Key Issues, IndiaCorpLaw (2023). A.Z.B. & Partners, Overview of the Bharatiya Nyaya Sanhita, 2023 (Jan. 2024).

[30] Bhatt & Joshi Associates, Electronic Evidence Under BSA 2023: Section 63 Certificate Requirements & Supreme Court Interpretation (2025).

[31] Ministry of Home Affairs, Reply to Lok Sabha Unstarred Question No. 265 (July 22, 2025) (India). Indian Cyber Crime Coordination Centre, Recent Cybercrime Trends in Financial Frauds (Aug. 12, 2024).

APPENDIX

Appendix A. Glossary of Key Web3 Terms

Term	Definition
Blockchain	A distributed, append-only ledger maintained by network consensus without a central administrator.
Wallet	Software or hardware generating and storing cryptographic keys; custodial (third-party held) or non-custodial (user held).
Smart contract	Self-executing code deployed on a blockchain that performs agreed steps automatically upon specified conditions.
DeFi	Decentralised finance — lending, borrowing and trading protocols operated through smart contracts without a financial intermediary.
NFT	Non-fungible token — a unique, non-interchangeable token representing ownership of a digital or physical asset.
DAO	Decentralised autonomous organisation — a member-governed entity whose rules are encoded in smart contracts.

VASP	Virtual asset service provider — an entity conducting exchange, transfer, custody or issuance-related services for virtual assets.

Table A1: Glossary of Key Web3 Terms

Appendix B. Cybercrime and Financial Fraud Statistics, India (2022–2024)

Year	NCRP Complaints Registered	Reported Financial Fraud Losses
2022	10,29,026 (10.29 lakh)	₹2,290.24 crore
2023	15,96,493 (15.96 lakh)	₹7,465.18 crore
2024	22,68,346 (22.68 lakh)	₹22,845.73 crore

Table B1: National Cyber Crime Reporting Portal Statistics, 2022–2024. Source: Ministry of Home Affairs, Reply to Lok Sabha Unstarred Question No. 265 (July 22, 2025).

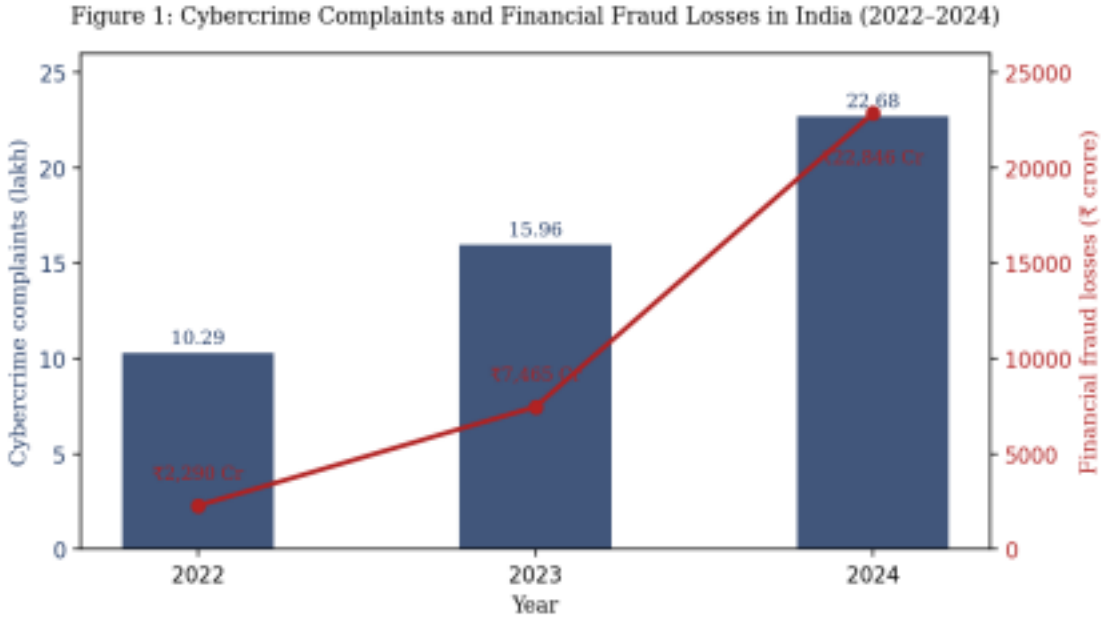


Figure 1: Cybercrime Complaints and Financial Fraud Losses in India, 2022–2024