Cryptocurrency Transactions and Financial Crime Detection in India: A Conceptual and Secondary Data Study

Sneha Niral Sharma
Assistant Professor
Anand Institute of Management & Information Science, MBA Department

Abstract: Cryptocurrency has emerged as a transformative financial innovation, enabling decentralized and borderless transactions. However, its pseudo-anonymous nature, cross-border accessibility, and limited regulatory clarity have increased its vulnerability to financial crimes such as money laundering, fraud, terrorist financing, and cyber-enabled scams. In the Indian context, the rapid growth of cryptocurrency adoption, coupled with evolving regulatory responses by institutions such as the Reserve Bank of India, Enforcement Directorate, and Financial Intelligence Unit – India, has created both opportunities and enforcement challenges.

This study adopts a conceptual and secondary data-based approach to examine the relationship between cryptocurrency transactions and financial crime detection in India. The research relies on secondary sources including government reports, regulatory notifications, published research articles, global crypto crime reports, and documented case studies of major cryptocurrency-related frauds. The study analyzes trends in crypto-enabled financial crimes, evaluates the adequacy of the current legal and regulatory framework, and explores the role of block chain forensic tools and Anti-Money Laundering (AML) compliance mechanisms in detecting illicit transactions.

The findings indicate that while block chain technology offers traceability advantages, regulatory fragmentation, technological gaps, and cross-jurisdictional issues continue to limit effective enforcement. The study proposes a conceptual framework linking transaction anonymity, regulatory oversight, forensic analytics, and enforcement outcomes to strengthen financial crime detection in India. The research contributes to policy discourse by recommending stronger compliance mechanisms, enhanced inter-agency coordination, and capacity building in block chain forensic investigation.

Keywords:- Cryptocurrency, Financial Crime, Block chain Forensics, Money Laundering, Crypto Regulation in India, AML Compliance, Cyber Financial Fraud, Financial Intelligence, Secondary Data Research, Conceptual Framework

Introduction:-

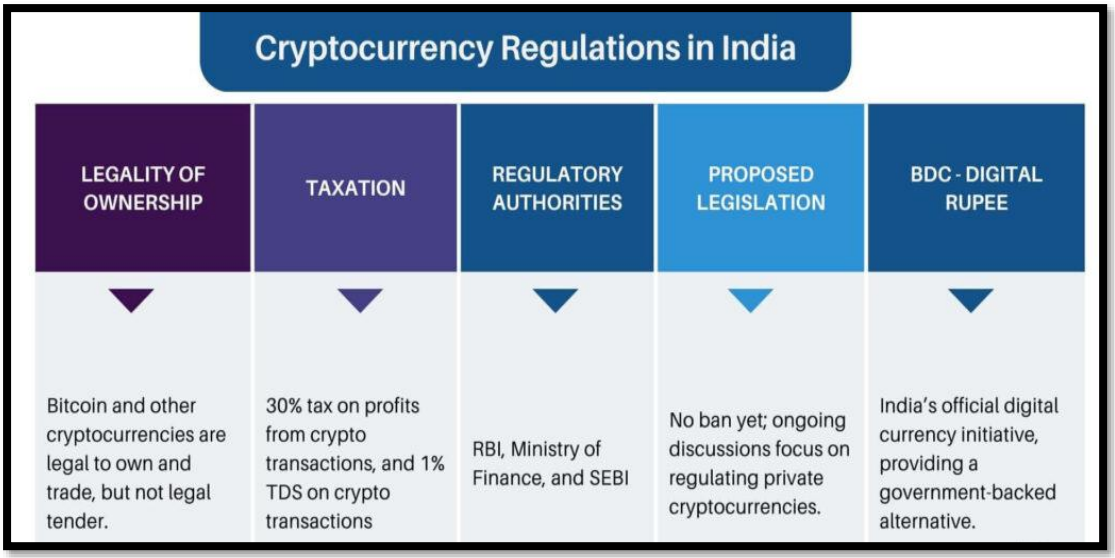
Cryptocurrency, often described as the "Wild West" of finance, is a digital asset that functions independently of traditional government or banking supervision. Unlike fiat currency issued and regulated by central authorities such as the Reserve Bank of India, cryptocurrencies operate on decentralized technological frameworks, primarily block chain. Block chain technology enables transactions to be executed, validated, and permanently recorded through a distributed ledger system without reliance on any central intermediary.

This decentralized structure enhances transparency and security through cryptographic mechanisms; however, it also presents regulatory and enforcement challenges. The pseudonymous nature of cryptocurrency transactions has created opportunities for misuse, making digital assets vulnerable to financial crimes such as cyber fraud, money laundering, darknet transactions, and illegal trade activities. In the Indian context, regulatory bodies including the Financial Intelligence Unit – India and enforcement agencies have increasingly emphasized monitoring virtual digital asset transactions to prevent illicit financial flows.

Globally, reports such as those published by the Federal Trade Commission indicate that consumers lost over $1 billion to crypto currency-related fraud between January 2021 and March 2022. A significant proportion of fraud-related payments were made in crypto currency, reflecting its growing use in scam

operations. Investment-related scams have been particularly prevalent, where fraudsters exploit urgency, scarcity, and promises of exceptionally high returns to attract unsuspecting investors. Many victims ultimately report complete loss of their invested capital.

In India, rapid



the adoption of crypto currency trading platforms and increasing digital payment penetration have raised concerns regarding regulatory oversight, tax compliance, and financial crime detection. The evolving legal framework, including anti-money laundering compliance requirements and reporting obligations for virtual asset service providers, reflects the government's attempt to balance technological innovation with financial security. This study, based on conceptual analysis and secondary data sources, aims to examine the patterns of crypto currency transactions in India, identify associated financial crime risks, and analyze the existing mechanisms for detection and regulatory control.

Literature Review

Cryptocurrency has attracted global attention not only as an innovative financial instrument but also as a medium for fraud, cybercrime, and illicit financial flows. Several international studies have examined the increasing association between cryptocurrency transactions and illegal activities. For instance, empirical analysis indicates that a measurable proportion of Bitcoin transactions have been linked to dark net markets, ransomware payments, and unlawful trade activities (Foley, Karlsen, & Putniņš, 2019). Similarly, research highlights how the pseudonymous and decentralized architecture of block chain networks can be exploited to conceal illicit financial transfers (Makarov & Scholar, 2020). These findings suggest that while block chain ensures transparency of transaction records, identifying the real-world identity behind wallet addresses remains a significant challenge.

Extensive research has also focused on the adaptation of Anti-Money Laundering (AML) frameworks to virtual assets. Traditional AML systems were designed for centralized banking institutions; however, cryptocurrency transactions operate across decentralized peer-to-peer networks. Scholars argue that AML compliance for digital assets requires enhanced Know Your Customer (KYC) protocols, block chain analytics tools, and real-time transaction monitoring mechanisms (Ahmed & Saeed, 2021). Earlier conceptual discussions on Bitcoin governance also emphasized regulatory and technological limitations in preventing illicit activity (Zohar, 2015). More recent literature suggests that integrating artificial intelligence and forensic block chain tracing tools can strengthen detection capabilities (Munn, 2021).

At the international policy level, the Financial Action Task Force has played a critical role in shaping global cryptocurrency regulation. The FATF (2019) introduced guidance for Virtual Asset Service Providers (VASPs), including the "Travel Rule," which mandates the sharing of originator and beneficiary information during digital asset transfers. Subsequent updates (FATF, 2021) emphasize risk-based approaches, cross-border cooperation, and regulatory harmonization to mitigate financial crime risks associated with virtual assets. These policy documents recognize the dual character of cryptocurrency as both a financial innovation and a potential tool for money laundering and terrorist financing.

In the Indian context, regulatory discussions have intensified following rapid growth in cryptocurrency trading activity. The Reserve Bank of India has expressed concerns regarding financial stability, investor protection, and systemic risks linked to private cryptocurrencies. Additionally, the inclusion of Virtual Digital Assets under anti-money laundering provisions has strengthened oversight mechanisms. Studies examining Indian taxation policies note that the imposition of a 30 percent tax on crypto gains and 1 percent TDS aims to enhance transparency and traceability of transactions (Gupta & Bose, 2022). Furthermore, the Financial Intelligence Unit – India has mandated reporting requirements for crypto exchanges to improve transaction monitoring and suspicious activity reporting.

Despite growing scholarly attention, gaps remain in the Indian academic landscape. Much of the existing research concentrates on investment behavior, market volatility, or technological aspects of block chain rather than evaluating financial crime detection systems. Limited empirical research assesses the operational challenges faced by enforcement agencies in tracing pseudonymous block chain transactions within India (Singh, 2023). Moreover, comparative studies analyzing the effectiveness of regulatory reforms before and after AML inclusion remain scarce. Therefore, there is a clear need for conceptual and secondary-data-based research that systematically evaluates crypto currency transaction patterns and financial crime detection mechanisms in India.

Objective of the research:-

1. To examine growth of crypto currency transactions in India.
2. **To study the regulatory framework governing crypto currency and Virtual Digital Assets (VDAs) in India,**
3. To evaluate the effectiveness of Anti-Money Laundering (AML) and Know Your Customer (KYC) mechanisms.

Research Methodology

This study adopts a **conceptual and descriptive research design** to examine cryptocurrency transactions and financial crime detection mechanisms in India. The research is based exclusively on **secondary data**, as the objective is to analyze existing regulatory frameworks, transaction trends, and financial crime patterns rather than collecting primary responses. The conceptual approach helps in understanding the theoretical foundations of cryptocurrency, block chain technology, and financial crime risks, while the descriptive design enables systematic interpretation of available data related to transaction growth, regulatory developments, and enforcement actions.

The study relies solely on **secondary data sources**, including official reports and publications from the Reserve Bank of India, notifications and policy documents issued by the Ministry of Finance, guidelines published by the Financial Intelligence Unit – India, and international compliance frameworks such as reports from the Financial Action Task Force. In addition, peer-reviewed research journals, academic publications, and annual reports of crypto currency exchanges have been examined to obtain relevant statistical and analytical insights.

For analysis, the study employs **trend analysis** to examine the growth and patterns of crypto currency transactions in India, **comparative analysis** to evaluate changes in regulatory measures over time, and **policy analysis** to assess the adequacy of existing financial crime detection mechanisms. Where numerical data is available, **descriptive statistical tools** such as percentage analysis and growth rate calculations are used to interpret transaction and fraud-related data.

This research design enables a comprehensive understanding of cryptocurrency-related financial risks and regulatory responses within the Indian context while maintaining a structured and evidence-based analytical framework.

Regulatory Framework in India

The regulatory framework governing cryptocurrency transactions in India has evolved significantly in recent years, particularly in response to concerns regarding financial crime, money laundering, tax evasion, and investor protection. Although crypto currencies are not recognized as legal tender in India, the government has introduced taxation provisions and anti-money laundering compliance requirements to regulate Virtual Digital Assets (VDAs) within the financial system.

One of the most significant regulatory developments was the introduction of a **30 percent tax on income arising from the transfer of Virtual Digital Assets,** announced in the Union Budget 2022 by the

Ministry of Finance. Under Section 115BBH of the Income Tax Act, gains from cryptocurrency transactions are taxed at a flat rate of 30 percent, without allowing set-off of losses against other income. In addition, a **1 percent Tax Deducted at Source (TDS)** under Section 194S is applicable on crypto transactions exceeding the prescribed threshold. These provisions aim to create a transparent reporting mechanism and enhance traceability of high-value digital asset transactions (Ministry of Finance, 2022).

Further strengthening oversight, the Government of India brought cryptocurrency exchanges and Virtual Asset Service Providers (VASPs) under the purview of the **Prevention of Money Laundering Act (PMLA), 2002** through a notification issued in March 2023. This move mandates crypto platforms to comply with Anti-Money Laundering (AML) and Know Your Customer (KYC) norms similar to those applicable to traditional financial institutions. Consequently, exchanges are required to maintain transaction records, verify customer identities, and report suspicious transactions to the Financial Intelligence Unit – India.

The **Financial Intelligence Unit – India (FIU-IND)** plays a central role in monitoring and analyzing financial transaction reports related to suspected illicit activities. Crypto exchanges operating in India are required to register with FIU-IND as reporting entities and comply with reporting obligations, including Suspicious Transaction Reports (STRs) and other compliance documentation. This registration requirement ensures that digital asset transactions are incorporated within the broader financial intelligence and surveillance ecosystem.

Additionally, the Reserve Bank of India has consistently emphasized concerns related to financial stability, consumer protection, and systemic risks associated with cryptocurrencies. While the RBI does not directly regulate cryptocurrencies as currency, it contributes to policy discussions and risk assessments related to digital assets and payment systems.

Enforcement agencies such as the Enforcement Directorate (ED), Income Tax Department, and cybercrime units have also intensified investigations into cryptocurrency-linked fraud, money laundering cases, and cross-border financial crimes. Their coordinated actions reflect the growing importance of integrating cryptocurrency transactions into India's financial crime detection framework.

Overall, India's regulatory approach reflects a shift from uncertainty toward structured oversight, combining taxation, AML compliance, reporting obligations, and enforcement measures. However, challenges remain in cross-border transaction tracing, technological capacity, and harmonization with global regulatory standards, thereby necessitating continued policy refinement and international cooperation.

Financial Crimes in Crypto currency

The rapid expansion of cryptocurrency transactions in India has created new avenues for financial innovation; however, it has simultaneously increased the risk of financial crimes due to the decentralized, pseudonymous, and borderless nature of block chain technology. The absence of a centralized monitoring authority and the complexity of tracing wallet addresses make cryptocurrencies attractive tools for illicit activities. The major types of financial crimes associated with cryptocurrency transactions in India are discussed below.

One of the most significant concerns is **money laundering**, where illegally obtained funds are converted into cryptocurrency to obscure their origin. Criminals exploit crypto exchanges, peer-to-peer platforms, and cross-border transfers to layer and integrate illicit funds into the financial system. With the inclusion of Virtual Digital Asset (VDA) service providers under the **Prevention of Money Laundering Act (PMLA), 2002**, regulatory authorities such as the Financial Intelligence Unit – India have strengthened monitoring mechanisms to detect suspicious crypto transactions.

Another prevalent issue is **Ponzi schemes**, where fraudulent operators promise exceptionally high and guaranteed returns on cryptocurrency investments. These schemes rely on funds from new investors to pay earlier participants, eventually collapsing when new inflows decline. Such schemes often misuse block chain terminology to appear technologically credible, misleading retail investors.

Closely related is **cryptocurrency investment fraud**, which includes fake trading platforms, impersonation scams, phishing attacks, and social media-based investment traps. Fraudsters frequently exploit limited investor awareness and the volatility of crypto markets to deceive individuals. Reports

from enforcement agencies indicate that investment scams constitute a major share of crypto-related financial losses.

Ransomware payments represent another critical financial crime category. In ransomware attacks, cybercriminals encrypt victims' data and demand payment in cryptocurrency due to its cross-border transferability and relative anonymity. This form of cyber extortion has increased globally and poses significant challenges for law enforcement agencies in tracing transactions across jurisdictions.

Cryptocurrencies are also used in **dark net transactions**, where illegal goods and services—including drugs, weapons, stolen data, and counterfeit documents—are traded on hidden online marketplaces. The encrypted and decentralized nature of block chain networks enables such transactions to bypass conventional financial surveillance systems.

Lastly, **tax evasion** has emerged as a growing concern in India. Some investors underreport or fail to disclose cryptocurrency gains to avoid taxation. Although the Government of India introduced a 30 percent tax on VDA gains and a 1 percent TDS mechanism under the Income Tax Act (2022), monitoring compliance remains challenging due to offshore exchanges and decentralized platforms. Agencies such as the Reserve Bank of India and enforcement bodies continue to emphasize the importance of transparency and reporting compliance.

Data Analysis & Discussion

This study relies on secondary data to analyse patterns in cryptocurrency adoption and associated financial crimes within the Indian regulatory context. The following section highlights key trends, comparative insights, and an evaluation of regulatory effectiveness.

Trend Growth of Crypto Adoption in India

Over recent years, cryptocurrency adoption in India has increased rapidly. Secondary data from industry reports and exchange platforms indicate a steady rise in the number of crypto investors, trading volumes, and registered wallets. This growth has been driven by factors such as increased digital literacy, widespread internet penetration, and the emergence of user-friendly applications enabling retail participation. Trend analysis suggests that the introduction of clearer regulatory policies, such as the virtual digital asset (VDA) tax regime and AML compliance requirements, has coincided with a surge in on-boarding retail and institutional participants. However, adoption growth has not been uniform, with periods of regulatory uncertainty—such as the proposed crypto ban in 2021—leading to temporary declines in trading volumes and exchange registrations.

Comparison of Fraud Cases before and After Regulation

Secondary data from government releases, enforcement agencies, and industry watchdog reports provide insight into fraud incidence before and after the introduction of structured regulations. Prior to the implementation of formal tax and AML guidelines in 2022–2023, India witnessed numerous high-profile scams, exchange collapses, and unregulated investment schemes, resulting in substantial financial losses to retail investors. Post-regulation data shows a relative decline in reported fraud cases attributable to increased monitoring by reporting entities and enhanced compliance requirements under the Prevention of Money Laundering Act (PMLA). Nonetheless, the persistence of sophisticated fraud vectors—such as phishing and Ponzi schemes indicates that regulatory frameworks have mitigated but not eliminated illicit activities. The trend comparison underscores the importance of ongoing enforcement and technological monitoring.

Global vs Indian Regulatory Framework

A comparative analysis of global and Indian frameworks reveals both convergence and divergence in regulatory approaches. Globally, jurisdictions such as the European Union and some Asian financial centres have adopted frameworks encompassing licensing, AML/CFT standards, wallet custody rules, and comprehensive disclosure requirements. India's regulations, particularly the 30 percent tax on crypto gains and the 1 percent TDS reporting requirement, reflect an emphasis on revenue realization and transparency. At the same time, the incorporation of crypto service providers under PMLA compliance aligns India with global anti-money laundering norms, as recommended by the Financial Action Task Force. However, India's regulatory model remains more cautious compared to some developed economies that have implemented dedicated digital asset regulatory sandboxes and licensing regimes.

The comparative evaluation highlights the evolving nature of crypto regulation and the need for harmonization with international best practices.

Effectiveness of AML Rules

Analysis of AML compliance effectiveness indicates that the extension of AML and KYC obligations to Virtual Asset Service Providers (VASPs) has improved transaction traceability and suspicious activity reporting in India. Data from the Financial Intelligence Unit – India reflects increased filings of Suspicious Transaction Reports (STRs) and proactive monitoring of cross-border fund flows. Trend analysis shows improved detection of laundering patterns involving decentralized finance (DeFi) protocols and peer-to-peer platforms. However, challenges persist due to the pseudonymous characteristics of block chain transactions and the use of privacy-enhancing technologies. Enforcement agencies continue to invest in block chain analytics tools and international cooperation mechanisms to track illicit transactions. The discussion suggests that while AML measures have strengthened the compliance landscape, their full effectiveness is contingent upon technological advancements and enhanced interagency coordination.

Finding

The study reveals a **significant rise in cryptocurrency adoption across India**, with millions of users holding virtual digital assets (VDAs) and crypto exchanges increasingly catering to retail investors, reflecting broader financial digitisation trends. However, this growth has been accompanied by a **substantial increase in fraud and cybercrime linked to crypto transactions**, including investment scams, laundering of illicit proceeds through stable coins like USDT, and sophisticated cross-border fraud networks that exploit decentralized platforms to evade detection and repatriate funds abroad. Regulatory developments, especially the inclusion of cryptocurrencies under the Prevention of Money Laundering Act (PMLA) and compulsory registration of VDA service providers with the Financial Intelligence Unit (FIU), have **strengthened oversight and reporting mechanisms**, resulting in an uptick in suspicious transaction reports and enforcement actions. Despite this, gaps in compliance enforcement and jurisdictional challenges persist, underscoring the **need for stronger forensic tools and block chain analytics** to trace pseudonymous transactions and link wallet activity to real-world entities. The research also highlights a **growing recognition among law enforcement and regulators of the dual nature of crypto** as both an innovation in financial services and a vector for organized financial crimes which has prompted collaborative efforts to improve AML/KYC standards and information-sharing frameworks. Finally, the findings point to **increasing international cooperation and policy alignment,** as India engages with global standards (e.g., FATF AML/CFT norms) to curb crypto-enabled crime while still promoting technological innovation in the financial sector.

Conclusion:

The study concludes that cryptocurrency has experienced rapid growth in India, driven by increasing digital adoption, fintech innovation, and rising investor interest in virtual digital assets. This expansion has positioned crypto as an emerging component of India's financial ecosystem. However, the growth has also been accompanied by significant financial crime risks, including money laundering, cyber fraud, Ponzi schemes, and cross-border illicit transactions. The pseudonymous and decentralized nature of block chain technology creates challenges for traditional enforcement mechanisms. Therefore, there is a strong need for advanced financial crime detection systems, including block chain analytics, forensic accounting tools, enhanced KYC/AML compliance, and stronger coordination between regulatory agencies and crypto exchanges. At the same time, regulatory frameworks must strike a careful balance between encouraging technological innovation and ensuring financial stability and consumer protection. A well-designed regulatory and forensic framework will help India harness the benefits of cryptocurrency while minimizing its misuse for financial crime.

References

1. Brenig, C., Accorsi, R., & Müller, G. (2015). Economic analysis of cryptocurrency-backed money laundering. Electronic Commerce Research, 15(2), 275–297.
2. Chainalysis. (2023). The 2023 crypto crime report: Trends in illicit cryptocurrency transactions. New York: Chainalysis Inc.

3. Financial Action Task Force (FATF). (2019). Guidance for a risk-based approach to virtual assets and virtual asset service providers. Paris: FATF.
4. Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies, 32(5), 1798–1853.
5. Kethineni, S., & Cao, Y. (2020). The rise in cryptocurrency scams and regulatory responses in India. Journal of Financial Crime, 27(3), 785–797.
6. Ministry of Finance, Government of India. (2023). Notification on inclusion of Virtual Digital Asset Service Providers under the Prevention of Money Laundering Act (PMLA), 2002. New Delhi: Government of India.
7. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 1(1), 1–9.
8. Reserve Bank of India (RBI). (2022). Financial stability report: Risks and implications of cryptocurrency adoption in India. Mumbai: RBI.