AG Publishing House

Investigative Frontiers Integration of Science Transforming Criminal Investigation

Year: 2026

Tracing the Digital Footprints: Blockchain Analysis and Cryptocurrency Crime Investigation

Ms. Gargi Pachuri[1]

[1]*Assistant Professor of Law Amity law School Amity University, Gwalior, Madhya Pradesh*

Abstract

Blockchain technology and cryptocurrencies have transformed the world of digital financial systems, providing decentralized, transparent, and secure digital transactions. Their widespread adoption has also made them easier to use for cybercrime activities like ransomware, money laundering, phishing, operating a darknet marketplace, investing and even terrorist financing. This review explores how blockchain analytics can be used to trace digital footprints, aiding cryptocurrency crime investigations. It covers the basics of the blockchain architecture, transactional operations of cryptocurrencies, as well as relevant forensics methods such as transaction graph analysis, wallet clustering, address attribution, and fund tracing. The review also describes some of the most common crimes involving cryptocurrencies, typical digital investigation processes, and the use of blockchain forensic tools. Finally, it has identified the technical hurdles associated with technologies that enhance privacy, legal and regulatory concerns in India, and trends like artificial intelligence-based blockchain analytics and cross-chain forensic investigations to improve the detection and digital forensic capabilities of cybercrime in the future.

[1] ISBN No. - 978-93-7640-081-2

Ms. Gargi Pachuri

Keywords; Blockchain Forensics; Cryptocurrency Crime; Blockchain Analysis; Digital Forensics; Cybercrime Investigation

1 Introduction

Blockchain technology and cryptocurrencies have revolutionized the global financial system by providing a decentralized, transparent, and borderless way to conduct transactions digitally. “Tracing the digital footprints" is a term used to describe the process of identifying, monitoring, and analyzing the permanent records of transactions that occur on blockchain networks. Public blockchains have immutable ledgers, meaning that each transaction is permanently recorded, unlike traditional financial systems. While cryptocurrencies like Bitcoin and Ethereum use pseudonymous wallet addresses, the blockchain history of these addresses can still be publicly viewed and traced to determine the flow of digital assets. This property has made blockchain a significant means of digital evidence in forensic investigations.[2]

Since Bitcoin was introduced in 2009, there has been a proliferation of cryptocurrencies and blockchain-based applications to address digital transactions, smart contracts, decentralized finance (DeFi) and cross-border transactions. As these technologies become more widely used by individuals, enterprises and financial institutions, they are also driving innovation and growth in the digital economy.[3]

The adoption of cryptocurrencies also harbors the potential for other types of cybercrime, such as ransomware, money laundering, darknet market trading, investment frauds, and cryptocurrency theft. Blockchain's decentralized nature, transaction speed, and global accessibility have posed serious obstacles to law enforcement agencies in the fight to track down criminals and freeze the proceeds of their crimes.[4]

This means that blockchain analysis is now an integral part of digital forensics and cybercrime investigations. By employing techniques such as transaction tracing, wallet clustering, and

[2] A. Singh, R. Jalota, and V. Gupta, “Blockchain Technology in Cryptocurrency: A Review,” in 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), 2022, pp. 715–719. doi: 10.1109/COM-IT-CON54601.2022.9850839.

[3] N. H. Hamzah, K. Osman, Q. W. Kong, A. M. Nasir, and N. M. M. Isa, “Forensic Analysis of Cryptocurrencies: A Comprehensive Overview Analisis Forensik Mata Wang Kripto: Tinjauan Komprehensif,” Asia-Pacific J. Inf. Technol. Multimed., vol. 14, no. 2, pp. 585–594, 2025, doi: https://doi.org/10.17576/apjitm-2025-1402-15.

[4] S. Shahi and S. Rath, “Cryptocurrency, Financial Fraud, and Regulatory Challenges,” 2026, pp. 167–187. doi: 10.1007/978-3-032-20889-7_9.

address attribution, investigators can follow the flow of cryptocurrency, identify suspicious activities, and establish links between blockchain addresses and real-world entities. Blockchain forensics is essential for successful investigations and fortifying digital financial systems in a field that continues to grow and advance with cryptocurrency-circulated crimes.

2 Fundamentals of Blockchain and Cryptocurrency Transactions

Blockchain technology is the backbone of cryptocurrencies, offering a secure, decentralized, and tamper-resistant digital transaction system. Unlike traditional financial systems with centralized authorities, blockchain employs a distributed ledger that is shared among many participants in the network, providing transparency, integrity, and immunity to unauthorized changes. The basic principles of the blockchain architecture and cryptocurrency transactions are vital for digital forensic investigators because they shape the creation, preservation, and reconstruction of digital evidence during cybercrime investigations.[5]

A. Blockchain Architecture

A blockchain is a distributed ledger made up of blocks of validated transactions that are stored sequentially. Every block has a timestamp, transaction details, a hash of the previous block, and a hash of the current block, forming an unchangeable record of blocks. If a previous block is modified, the hash changes and it invalidates the next block in the chain, which means that the transactions are easily recognizable as not originating from the proper chain. Consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) allow nodes to agree on the transactions that are included on the blockchain without relying on a central authority and ensure that only verified transactions are added to the blockchain.[6]

B. Cryptocurrency Wallets and Transaction Process

The ownership of a cryptocurrency is determined by a pair of cryptographic keys: a secret key and a public key. The public key is used to create wallet addresses for receiving digital assets, while the private key is what enables transactions and must be kept confidential. Most cryptocurrency transactions start with a private key signing the transaction, broadcasting it to the network of nodes that validate it based on the consensus algorithm. Upon confirmation, the

[5] S. Arif, M. Iqbal, and D. S. E. Y. Qadeem, “Role Of Cryptocurrency And Blockchain Technology In Modern Financial Markets,” Qual. Res. J. Soc. Stud., vol. 3, no. 1, pp. 804–816, 2026, doi: 10.63878/qrjs947.

[6] G. Kacheru, “Blockchain Technology: Architecture, Applications, and Challenges,” Turkish J. Comput. Math. Educ., vol. 09, no. 3, pp. 1433–1438, 2018, doi: https://doi.org/10.61841/turcomat.v9i3.14965.

deal is settled and inscribed on the blockchain in an unalterable record, which can be analyzed by investigators later.[7]

C. Transparency and Pseudonymity in Blockchain

Public blockchains are transparent as every transaction that's confirmed is permanently visible to everyone on the network. But users aren't actually anonymous, they are represented by alphanumeric wallet addresses instead. It is especially relevant in the context of forensic investigations, where investigators can use the blockchain's transaction history to identify a group of wallet addresses, open-source intelligence, and exchange records to tie digital transactions to a person or organization.[8]

Table 6: A comparison of key aspects of a traditional database versus a blockchain[9]

Aspect	Traditional Database	Blockchain
Control	Uses client-server network architecture on a central server.	Consists of several decentralised nodes, each participating in administration and verifying new data into the blockchain.
Security	Can be compromised depending on the infrastructure of the database administrator.	Data is stored in a decentralised manner that builds security into its structure, and uses cryptographic techniques to make it tamper-proof.
Integrity of Data	Can be altered, corrupted, or deleted by anyone with access to the database.	Immutable. Majority of nodes must reach consensus, which guarantees the security of the network, making it tamper-proof. Past entries on the blockchain cannot be changed.
Transparency	Private or depending on the settings of the centralised network.	Pseudo-anonymous. Public blockchains, like Bitcoin, are transparent, meaning anyone can see the transaction history. Advanced cryptographic techniques like zero-knowledge proofs (ZKPs) and confidential transactions can hide transaction details while maintaining the integrity of the blockchain.

[7] N. Gowda and C. Chakravorty, "Comparative study on cryptocurrency transaction and banking transaction," Glob. Transitions Proc., vol. 2, pp. 530–534, 2021, doi: https://doi.org/10.1016/j.gltp.2021.08.064.

[8] J. Sedlmeir, J. Lautenschlager, G. Fridgen, and N. Urbach, "The transparency challenge of blockchain in organizations," Electron. Mark., vol. 32, pp. 1779–1794, 2022, doi: https://doi.org/10.1007/s12525-022-00536-0.

[9] H. K. Gill, "The Importance of Blockchain Forensics Investigations in the Digital Ecosystem (with a focus on Cryptocurrency)," SSRN, pp. 1–21, 2024, doi: http://dx.doi.org/10.2139/ssrn.5237438.

Recording of Data	Four functions can be performed on data: create, read, update, and delete (CRUD).	A user can only add more data in the form of additional blocks. All previous data is permanently stored and cannot be altered. The only operations associated with blockchains are read and write.

3 Blockchain Analysis Techniques for Digital Investigation

Blockchain analysis involves a collection of forensic methods that analyze cryptocurrency transactions, uncover suspicious financial activities, and trace the flow of digital assets through blockchain networks. The permanent and transparent nature of blockchain transactions on most cryptocurrency platforms makes it possible for investigators to use analysis to determine relationships between wallet addresses, recognize suspicious transaction patterns and link blockchain activity with entities in the real world. These techniques are essential in ransomware, fraud, money laundering and darknet market investigations.[10]

- **Transaction Graph Analysis:** Transaction graph analysis depicts blockchain transactions as nodes and links, with wallet addresses forming the nodes and the transactions themselves forming the links. Investigators can analyze these transaction networks to look for transaction patterns, asset movement and unusual patterns that could indicate an illegal activity.
- **Wallet Clustering Techniques:** Wallet clustering aggregates and correlates a set of wallet blockchain addresses that appear to belong to the same wallet or organization. Common-input ownership and change-address detection are heuristic techniques that help investigators assemble wallets to reconstruct the contents of user-controlled wallets and increase their understanding of transaction networks.
- **Address Attribution and Entity Identification:** Address attribution is the process of associating a specific wallet address on the blockchain with an identifiable entity, like a cryptocurrency exchange, darknet markets, ransomware groups, or even a user. These associations are made using blockchain transaction data, exchange records, open-source intelligence (OSINT), and public data sets.
- **Flow-of-Funds (Fund Tracing):** Fund tracing entails tracking the path of cryptocurrency from its source to its final destination. There are numerous applications

[10] S. Johri, "Strengthening Digital Forensics with Blockchain Technology and Algorithms," World J. Adv. Res. Rev., vol. 24, pp. 459–467, 2024, doi: https://doi.org/10.30574/wjarr.2024.24.2.3317.

that use this technique to detect laundering patterns, track stolen funds, and trace transactions through mixers, exchanges, or cross-chain services to uncover movements of illegal funds.

- **On-Chain Analytics and Visualization Methods:** On-chain analytics involves an analysis of on-chain data including transaction metadata, wallet interactions, and network activity to identify suspicious transactions. Visualization tools, like transaction graphics and network diagrams, help to demystify complex blockchain interactions and allow investigators to comprehend vast amounts of transactions more easily.
- **Blockchain Forensic Tools:** Commercial blockchain forensics platforms like Chainalysis, CipherTrace, TRM Labs and Elliptic add features like transaction tracing, wallet attribution, risk scoring and visualization to blockchain forensics. These tools help financial institutions and law enforcement to detect and flag suspicious cryptocurrency activity and aid in digital forensic investigations, while significantly boosting the efficiency of blockchain intelligence analysis.

4 Cryptocurrency Crimes and Investigation Process

As cryptocurrencies become more prevalent, they are opening up novel avenues for financial innovation and offering a larger area for cyber-criminal activities. Blockchains are decentralized, transactions are fast and happen across borders, and everyone using the blockchain operates under a pseudonym – all of which have driven criminals to embrace cryptocurrencies as an appealing option when it comes to hiding out on the darknet. As a result, law enforcement agencies have incorporated blockchain forensics into their digital investigations to catch perpetrators, track illegal transactions, and recover stolen assets. It is crucial that a digital forensic professional is aware of the various types of crimes facilitated by cryptocurrencies and the typical investigation procedure.[11]

A. Major Cryptocurrency-Enabled Crimes

The following are the most common crimes involving cryptocurrencies:

- **Ransomware attacks:** Ransom demands are paid in cryptocurrencies, most commonly in Bitcoin or a more private option, as they are easily accessible worldwide and relatively hard to trace.

[11] D. D. Khan, H. Farman, S. Hassan, M. Seelro, and M. H. Mughal, "Cryptocurrency Crimes: A Systematic Literature Review of Bitcoin's Role in Illicit Activities," Pakistan J. Eng. Technol. Sci., vol. 12, no. 01, pp. 12–25, 2024, doi: https://doi.org/10.22555/pjets.v12I1.1121.

- **Money laundering:** Illegal money is then hidden in a series of cryptocurrency exchanges, cryptocurrency mixers, decentralized exchanges or cross-chain bridges and then changed back into fiat.
- **Darknet marketplace transactions:** Cryptocurrencies are also popular choices at illegal online marketplaces that are hosted on anonymous networks, which are used to buy and sell illegal drugs, weapons, fake documents, stolen data, and other illegal items.
- **Phishing attacks:** Fraudsters impersonate trusted organizations or cryptocurrency platforms to obtain victims' wallet credentials, private keys, or recovery phrases and subsequently steal digital assets.
- **Investment scams and fraud:** Criminals are creating fake investment schemes, fake initial coin offerings (ICOs), Ponzi schemes, rug pulls, and impersonation scams to defraud investors and steal their money.
- **Terrorist financing:** There have been some instances of extremist groups trying to raise funds via cryptocurrencies or moving money across borders without going through traditional banking channels, though the amount is fairly small compared to traditional fundraising methods.

A cryptocurrency investigation generally follows a structured forensic process:

- **Evidence collection:** Maintain the integrity of digital evidence and the chain of custody of all evidence recovered from computers and mobile devices, cryptocurrency wallets, cloud-based storage, browser history, and communication platforms.
- **Blockchain tracing:** Specific blockchain analytics tools are used to trace transaction histories, follow transaction paths, and track the flow of digital assets on blockchain networks.
- **Wallet identification:** Wallet clustering techniques, address attribution, open-source intelligence (OSINT), and known address databases are used to correlate wallet addresses with exchanges, organisations or individual users.
- **Exchange data acquisition:** The investigation involves collecting Know Your Customer (KYC) records, account registration details, IP logs, transaction histories, and withdrawal information from regulated exchanges via legal processes to identify suspects.
- **Documentation and reporting:** The investigation ends with extensive documentation of analytical methods, timelines of transactions, findings of evidence, visual transaction graphics and expert interpretation. Such reports shall be technically accurate, repeatable and appropriate for presentation in court.

B. Standard Investigation Workflow

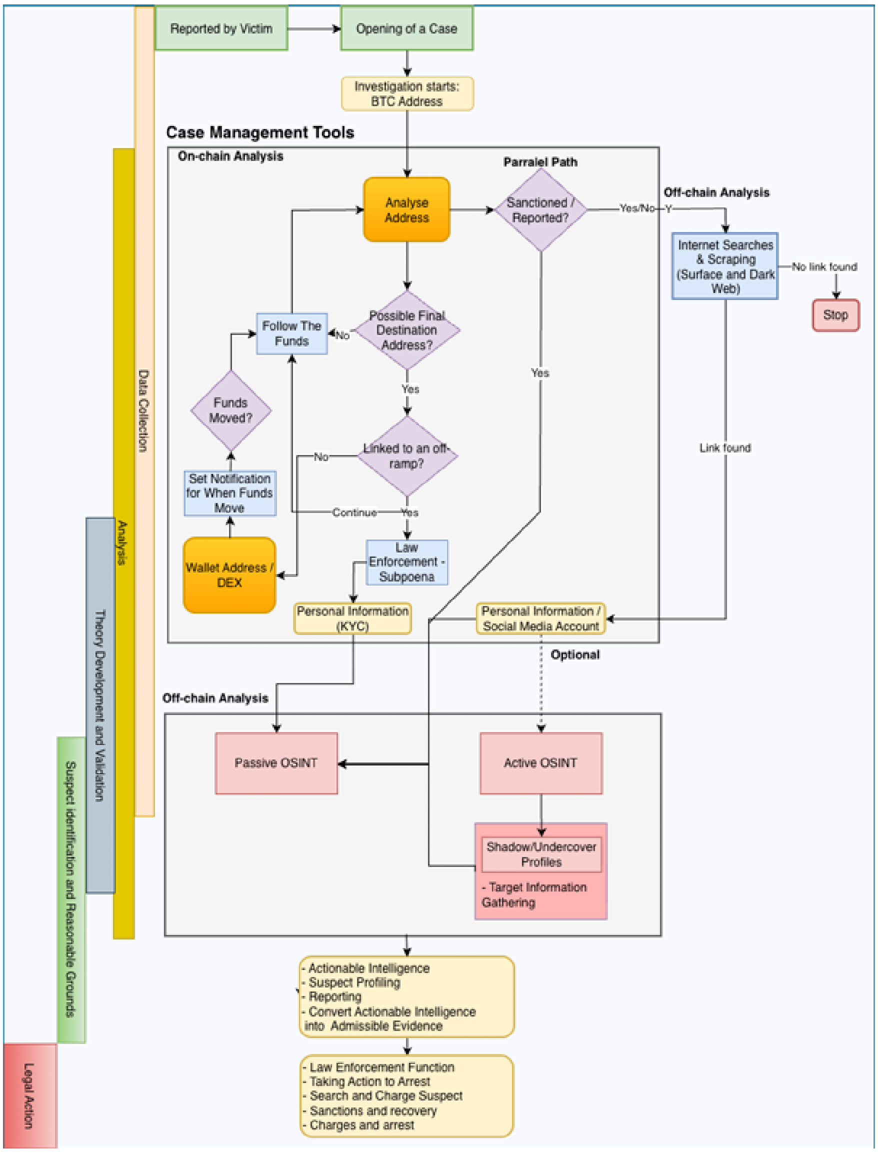

Figure 15: Process for Conducting Cryptocurrency Crime Investigations[12]

[12] J. Botha, K. Singh, and L. Leenen, “Evaluating an Investigative Process for Cryptocurrency-Related Crimes,” Int. Conf. Cyber Warf. Secur., pp. 45–56, 2026, doi: 10.34190/iccws.21.1.4538.

By combining blockchain analytics with traditional digital forensic techniques, investigators are able to find cryptocurrency-related crimes, connect suspects with digital assets, and build a case for successful prosecution.

5 Challenges, Legal Issues, and Future Directions

Blockchain investigations are grappling with highly technical, legal, and regulatory difficulties given the growing sophistication of cryptocurrency ecosystems. While the transparency of blockchain records can benefit privacy, new technologies are being developed to maintain privacy and decentralized finance services do not make it easy to identify offenders and trace illegal funds. These are exacerbated in India due to changing regulation and cross-border transactions, and the need for increased international cooperation.

A. Challenges

There are several technical challenges with blockchain investigations. Monero and Zcash are privacy-focused cryptocurrencies that use powerful cryptographic methods like ring signatures, stealth addresses and zero-knowledge proofs to obscure transaction details, making it much harder to trace transactions. Similarly, cryptocurrency mixers, tumblers, cross-chain bridges, and decentralized finance (DeFi) platforms also help obscure the source and final destination of digital assets by breaking up and sending coins through many different blockchain networks. These technologies make it harder to blockchains successfully using traditional approaches, necessitating improved blockchain forensic skills and cross-chain analysis.[13]

B. Legal Issues in India

India does not have a specific cryptocurrency law in place, rather, virtual digital assets are regulated by a mix of tax provisions, anti-money laundering laws, and the existing cybercrime legislation. Under the Prevention of Money Laundering Act (PMLA), 2002, Virtual Asset Service Providers (VASPs) including cryptocurrency exchanges are now covered and must keep records of Know Your Customer (KYC) and follow monitoring procedures for suspicious transactions and report them to the Financial Intelligence Unit–India (FIU-IND). Issues still exist

[13] S. Dyson, W. J. Buchanan, and L. Bell, "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime," JBBA, vol. 1, no. 2, pp. 1–6, 2018, doi: https://doi.org/10.31585/jbba-1-2-(8)2018.

for jurisdiction over cross-border transactions, gathering evidence from foreign exchanges, and the admissibility and preservation of blockchain-based digital evidence in criminal cases.[14]

C. Future Directions

AI-powered blockchain analytics, machine learning, and automated transaction monitoring will become integral tools for future blockchain investigations in India to uncover suspicious financial patterns more efficiently. Cross-chain forensic investigation techniques will enhance investigators' capacity to trace assets that move between various blockchain networks and decentralized platforms. Improved international cooperation, including through the FATF recommendations, MLATs and cooperation between Indian law enforcement agencies and global cryptocurrency exchanges, will further facilitate investigation and prosecution of cryptocurrency based crimes and foster a safe and transparent cryptocurrency financial ecosystem.[15]

6 Conclusion

Blockchain technology has revolutionized digital financial transactions by creating transparency, immutability, and decentralization, and introduced new challenges for cybercrime investigations. Blockchain analysis has become an essential tool in digital forensics, helping investigators to track transactional movements, connect wallet owners, and determine the evidentiary ties between digital assets and criminal activities, as cryptocurrency crimes continue to develop. Investigation techniques like transaction graph analysis, wallet clustering, address attribution and fund tracing greatly improve investigative capabilities. However, the use of privacy-oriented cryptocurrencies, mixers, cross-chain bridges and the Decentralized Finance (DeFi) sector still complicates the tracking of illicit funds. The regulatory developments in the Indian context under the anti-money laundering frameworks and enhanced compliance norms are significant strides in the governance of cryptocurrencies. With improvements in AI, machine learning, cross-chain forensic tools, and international partnerships and legislation, investigations on blockchain will become more effective and the digital financial ecosystem can continue to flourish safely.

---

[14] P. Kumari, "Cryptocurrency Regulation in India: Legal Uncertainty, Financial Stability, and Digital Sovereignty," Minnesota J. Bus. Law Entrep., pp. 1466–1476, Feb. 2026, doi: 10.52783/mjble.440.

[15] H. F. Atlam, N. Ekuri, M. A. Azad, and H. S. Lallie, "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions," Electronics, vol. 13, no. 3568, 2024, doi: https://doi.org/10.3390/electronics13173568.

7 Reference

[1] A. Singh, R. Jalota, and V. Gupta, “Blockchain Technology in Cryptocurrency: A Review,” in 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), 2022, pp. 715–719. doi: 10.1109/COM-IT-CON54601.2022.9850839.

[1] N. H. Hamzah, K. Osman, Q. W. Kong, A. M. Nasir, and N. M. M. Isa, “Forensic Analysis of Cryptocurrencies: A Comprehensive Overview Analisis Forensik Mata Wang Kripto: Tinjauan Komprehensif,” Asia-Pacific J. Inf. Technol. Multimed., vol. 14, no. 2, pp. 585–594, 2025, doi: https://doi.org/10.17576/apjitm-2025-1402-15.

[2] S. Shahi and S. Rath, “Cryptocurrency, Financial Fraud, and Regulatory Challenges,” 2026, pp. 167–187. doi: 10.1007/978-3-032-20889-7_9.

[3] S. Arif, M. Iqbal, and D. S. E. Y. Qadeem, “Role Of Cryptocurrency And Blockchain Technology In Modern Financial Markets,” Qual. Res. J. Soc. Stud., vol. 3, no. 1, pp. 804–816, 2026, doi: 10.63878/qrjs947.

[4] Kacheru, “Blockchain Technology: Architecture, Applications, and Challenges,” Turkish J. Comput. Math. Educ., vol. 09, no. 3, pp. 1433–1438, 2018, doi: https://doi.org/10.61841/turcomat.v9i3.14965.

[5] N. Gowda and C. Chakravorty, “Comparative study on cryptocurrency transaction and banking transaction,” Glob. Transitions Proc., vol. 2, pp. 530–534, 2021, doi: https://doi.org/10.1016/j.gltp.2021.08.064.

[6] J. Sedlmeir, J. Lautenschlager, G. Fridgen, and N. Urbach, “The transparency challenge of blockchain in organizations,” Electron. Mark., vol. 32, pp. 1779–1794, 2022, doi: https://doi.org/10.1007/s12525-022-00536-0.

[7] K. Gill, “The Importance of Blockchain Forensics Investigations in the Digital Ecosystem (with a focus on Cryptocurrency),” SSRN, pp. 1–21, 2024, doi: http://dx.doi.org/10.2139/ssrn.5237438.

[8] S. Johri, “Strengthening Digital Forensics with Blockchain Technology and Algorithms,” World J. Adv. Res. Rev., vol. 24, pp. 459–467, 2024, doi: https://doi.org/10.30574/wjarr.2024.24.2.3317.

[9] D. Khan, H. Farman, S. Hassan, M. Seelro, and M. H. Mughal, “Cryptocurrency Crimes: A Systematic Literature Review of Bitcoin’s Role in Illicit Activities,” Pakistan J. Eng. Technol. Sci., vol. 12, no. 01, pp. 12–25, 2024, doi: https://doi.org/10.22555/pjets.v12I1.1121.

[10] Botha, K. Singh, and L. Leenen, “Evaluating an Investigative Process for Cryptocurrency-Related Crimes,” Int. Conf. Cyber Warf. Secur., pp. 45–56, 2026, doi: 10.34190/iccws.21.1.4538.

[11] S. Dyson, W. J. Buchanan, and L. Bell, “The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime,” JBBA, vol. 1, no. 2, pp. 1–6, 2018, doi: https://doi.org/10.31585/jbba-1-2-(8)2018.

[12] P. Kumari, “Cryptocurrency Regulation in India: Legal Uncertainty, Financial Stability, and Digital Sovereignty,” Minnesota J. Bus. Law Entrep., pp. 1466–1476, Feb. 2026, doi: 10.52783/mjble.440.

[13] F. Atlam, N. Ekuri, M. A. Azad, and H. S. Lallie, “Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions,” Electronics, vol. 13, no. 3568, 2024, doi: https://doi.org/10.3390/electronics13173568.