Asian Journal
of Criminal Justice
and Forensic Studies

Vol. 2 | No. 1 | 2026
Journal homepage: https://asianjustice.kz/

UDC 343.98 : 004.75
DOI: 10.63621/ajcjfs/1.2026.76

Article's History:
Received: 20.10.2025; Revised: 03.02.2026; Accepted: 18.03.2026

The use of blockchain technologies in the investigation of cybercrimes in India and Vietnam

Aigerim Shegebaeva*
Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Kazakhstan
https://orcid.org/0009-0002-2533-8553

Suggest Citation:
Shegebaeva, A. (2026). The use of blockchain technologies in the investigation of cybercrimes in India and Vietnam. *Asian Journal of Criminal Justice and Forensic Studies*, 2(1), 76-88. doi: 10.63621/ajcjfs/1.2026.76.

Abstract. The aim of the study was to determine the level of effectiveness of digital forensics of virtual assets in law enforcement practices in India and Vietnam. The methodology was based on the conceptual-methodological method, regulatory and legal analysis, scenario-typological classification, case-study, and structural-logical modelling. It has been established that assessing the effectiveness of blockchain forensics should be based not only on on-chain analysis tools, but also on the complete operational chain of actions of the authority (artifact collection → on-chain analysis → identification of intermediaries → procedural actions → international cooperation → evidence formalisation). The effectiveness of blockchain forensics was operationalised through the metrics of asset restraint/recovery, disruption, attribution leverage, evidentiary robustness, and time-to-intervention. The presence of Anti-Money Laundering mechanisms and procedural procedures was a key condition for the transition from technical tracing to property measures and proving in criminal proceedings. It has been observed that in Indian practice, the main emphasis was placed on property results, which allowed for the seizure of assets worth approximately 1,646 crore rupees in the BitConnect case and the freezing of over 77 BTC in the E-Nuggets case. The success of investigations was ensured by a rapid transition from transaction analysis to interaction with exchanges, which effectively restricts criminals' access to crypto assets. Vietnamese investigations focus on large-scale investment pyramids, where losses amounted to nearly 10 trillion dong and over 51 million USDT. Effectiveness in these cases was manifested through the complete shutdown of fraudulent platforms and the detention of organisers, achieved by combining on-chain payments with digital traces in accounts and logs. Evidentiary robustness requires formalised procedures concerning the data source, reproducibility, and the chain of custody, as well as a standardised sequence of actions: "on-chain tracing → establishment of a control point (Virtual Asset Service Provider / device) → procedural action". The practical significance lies in the implementation of the results in the activities of law enforcement agencies, the judiciary, and the educational process to enhance the effectiveness of combating offences in the digital sphere

Keywords: evidence; data; on-chain; assets; effectiveness; route

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

Introduction

The proliferation of crypto assets and services based on blockchain technologies has transformed the nature of cybercrime: phishing, investment fraud, extortion, and money laundering combine off-chain infrastructure (pseudo-platforms, communication channels, affiliate networks) with an on-chain payment layer, within which transactions pass through public ledgers, stablecoins, and exchange services. In such circumstances, the blockchain serves as a source of data relevant to the investigation; however, its practical value depends on the procedural conversion of technical findings into admissible evidence and legal consequences. On-chain tracing without off-chain verification and proper documentation of digital artifacts generally fails to yield a legally robust outcome. A critical aspect was understanding how law enforcement agencies apply blockchain tools in actual cases and which factors determine the effectiveness of such practices in different jurisdictions, particularly in India and Vietnam.

The existing scholarly discourse on India was viewed through the lens of policy development and research trends in the field of cryptocurrencies and Distributed Ledger Technology (DLT). The work of K. Ghosh & P.K. Das (2025) demonstrated that the regulatory framework and institutional responses to virtual digital assets influence how the research and applied agenda concerning risks, compliance, and control was shaped. This underscores that political and regulatory approaches act as a "multiplier" of law enforcement capabilities but do not, in themselves, guarantee the reproducibility of evidentiary conclusions in criminal cases. In the realm of India's legal challenges, D. Halder & A. Saiyed (2022) established that cryptocurrency offences have a victimological dimension: low user awareness and regulatory gaps increase victim vulnerability and contribute to the mass involvement of victims in investment fraud schemes. This explains the socio-legal prerequisites for the spread of crypto-investment fraud and highlights the need for evidentially robust investigation procedures that combine on-chain tracing with off-chain verification and proper documentation of digital evidence.

In a study by P. Seerwani & M.P. Ram Mohan (2025), it was found that Virtual Asset Service Providers (VASPs) act as institutional "control points" through which technical on-chain data can be linked to identifying information, compliance obligations, and legal procedures. This approach substantiates why the effectiveness of blockchain forensics in investigative practice depends on access to VASP data and the ability to convert on-chain tracing into procedural decisions (data requests, freezing/seizure, evidentiary formalisation). F. Prakash & H. Sadawarti (2022) established that the use of blockchain approaches in the chain of custody model enhances the integrity, traceability, and change control of digital evidence, reducing the risk of substitution or loss of evidentiary information during its handling and transfer. This supports the thesis that "on-chain ↔ off-chain" integration must be accompanied by standardised procedural documentation of artifacts; otherwise, technically correct conclusions do not ensure sufficient evidentiary robustness.

Scholarly sources from Vietnam primarily emphasise the nature of fraudulent ecosystems and the procedural requirements for digital evidence. Transnational scam schemes, according to the work of H.T. Luong & H.M. Ngo (2024), were characterised by a resilient organisational structure and adaptive monetisation models, which complicate their termination within a single jurisdiction and necessitate inter-agency and international coordination. This explains why, in cases with "off-chain" dominance, investigation effectiveness depends on rapid access to digital traces and procedures for interaction with infrastructure providers and foreign partners, not solely on on-chain tracing. Research by T.T.T. Nguyen (2025) showed that in Vietnamese criminal proceedings, the effectiveness of working with digital evidence was determined by compliance with standards of admissibility, reproducibility, and proper documentation, which directly influence the judicial assessment of technical findings. This means that blockchain analytics acquires evidentiary value only under the condition of procedurally correct documentation and the integration of on-chain data with off-chain sources (accounts, logs, devices); otherwise, technically substantiated claims remain procedurally vulnerable.

In the context of Kazakhstan, Y. Saniyazova *et al.* (2024) established that the institutionalisation of digital forensics in Kazakhstan enhances the capacity of law enforcement agencies to investigate cybercrimes through the systematic use of digital traces, expert methodologies, and appropriate infrastructure. The authors emphasised that even with technically available data (digital artifacts of financial transactions), effectiveness was determined by the procedural quality of evidence collection, preservation, and interpretation. The effectiveness of combating internet fraud, as shown in the work of S. Shaisultanov *et al.* (2024), largely depends on the coherence of investigative operations with the procedural formalisation of their results and the timeliness of obtaining data from intermediaries and services. This reinforces the thesis regarding the necessity of a clear sequence: "detection of a digital trace → establishment of a control point → procedural action", which was analogous to the approach for converting on-chain findings into legally significant outcomes. T. Simbayev (2025) noted that mechanisms for the confiscation of digital assets without a conviction give rise to specific legal and procedural challenges concerning the proof of criminal origin, ensuring proper asset control, and adhering to property rights guarantees. Even with successful tracing of fund movements, the final outcome (freezing/seizure/confiscation) depends on the legal basis and procedural standards, not solely on the technical reconstruction of transactions.

Existing studies have mainly focused on either the regulatory and legal aspects of the cryptosphere or general issues of digital evidence, but have not sufficiently explained how on-chain tracing translates into procedurally and

legally robust results through integration with off-chain data and "control points" (primarily VASPs). Therefore, the aim of the study was to evaluate the use of blockchain technologies to combat cybercrime in India and Vietnam. To achieve this goal, the following tasks were set: to operationalise the assessment of the effectiveness of blockchain forensics in cyber investigations, analyse publicly documented cases of cybercrime in India and Vietnam, and develop guidelines for standardising procedures based on the identified limitations of on-chain analytics to minimise the loss of evidence and increase the evidentiary robustness of conclusions.

Materials and Methods

The research was conducted using a comprehensive approach that combined conceptual-methodological analysis, scenario-typological classification of typical cryptocurrency crime scenarios, regulatory and legal analysis of the legal frameworks of India and Vietnam, a case study of five publicly documented cases from official law enforcement communications, and structural-logical modelling to assess the transition from on-chain analysis to procedural outcomes. Through the method of conceptual-methodological analysis, the content of blockchain/cryptocurrency forensics was clarified, and basic analytical constructs were defined (transaction graph, address clustering, the distinction between "address/wallet", the role of VASPs and off-chain sources). This was done to substantiate which specific data and artefacts were relevant for forensics and which assumptions (including probabilistic ones) require explicit documentation and verification. Using the scenario-typological classification method, typical cryptocurrency crime scenarios were systematised – investment scam/Ponzi, pseudo-exchanges/pseudo-Decentralised Exchanges (DEX), stablecoin payments, ransomware – with the recording of their on-chain/off-chain indicators, typical limitations/countermeasures, and key evidentiary requirements. This approach enabled the unification of interpretation and the linking of technical procedures (tracing, clustering, interaction with VASPs, seizure of artefacts) with procedural requirements (chain of custody, reproducibility, procedural data requests). The aforementioned scenarios were selected as representative because they reflect the most common models of criminal monetisation and differ in the ratio of on-chain/off-chain components and the role of infrastructural control points, allowing for a comparison of the conditions for "converting" analysis into a procedural outcome. The selection criteria were the presence of repeatable analytical features suitable for coding, relevance to performance metrics (attribution leverage, disruption, asset restraint/recovery, evidentiary robustness), and the practical significance of evidentiary requirements for law enforcement interaction with VASPs and infrastructure providers. This enabled the formation of a unified coding scheme suitable for subsequent effectiveness assessment using operationalised metrics.

Using the regulatory-legal method, the legal framework for qualifying cybercrimes and handling digital evidence in the jurisdictions of India and Vietnam was analysed. These jurisdictions were chosen due to their different models of concluding investigations and, consequently, the different conversion of on-chain analysis into outcomes: in India, property measures (freeze/seizure/attachment) predominate; in Vietnam, disruption and arrests in cases where the off-chain component dominates. For India, the Act of the Information Technology No. 21 (2000), The Prevention of Money-Laundering Act No. 15 (2003), and the official report (press release) of the CoinDesk (2025) were analysed. For Vietnam, the Criminal Procedure Code No. 101 (2015), the Law on Cybersecurity No. 24 (2018), and the Anti-Money Laundering Law No. 14 (2022) were examined. These documents were selected as framework sources that define access to digital data, Anti-Money Laundering (AML)/property measures concerning crypto-assets, and procedural evidentiary requirements, and also reflect the practice of their application in documented cases. This was done to establish which specific norms and institutional powers in India and Vietnam enable or limit the transformation of on-chain analysis results into procedurally significant actions (obtaining/securing evidence and property measures concerning crypto-assets and individuals).

To systematise and analyse the technical and procedural parameters of the practical application of blockchain technologies and assess their effectiveness, the case-study method was applied to five publicly documented cybercrime cases: E-Nuggets (India Today, 2022) and the BitConnect (CoinDesk, 2025) cases in India. Also included were Winrich/Wintop (Ho Chi Minh City Public Security Department, 2021), Matrix Chain (MTC) (Ministry of Public Security, 2025a), and KAYPLE (Ministry of Public Security, 2025b) in Vietnam. The selection was determined by the presence of a clear crypto component (Bitcoin (BTC)/Tether (USDT), VASPs) and the possibility to compare the Indian model of property measures with the Vietnamese model of disruption. The choice of these specific cases was due to their representativeness: they involve complex transaction routes, specific fraudulent platform models, and significant scales of losses. The analysis was performed by comparing the cases based on the role of crypto/on-chain routes, off-chain control points (VASPs/devices/accounts), procedural actions, and the level of evidentiary value. This allowed for an assessment of the actual conversion of technical tracing into legal consequences (asset seizure, arrests, scheme disruption) under different national law enforcement models.

Using the method of structural-logical modelling, a system of five operationalised metrics was presented – asset restraint/recovery, disruption, attribution leverage, evidentiary robustness, time-to-intervention – and a structural-logical model of the operational chain was developed following the scheme "on-chain tracing → identification of control point (VASP/custodian/device) → procedural action". The selection of these indicators was due to their ability to encompass the entire operational chain of actions

from detection to asset recovery, their established status in the scientific literature on digital forensics, which ensures the validity of the analysis, and allows for distinguishing between the jurisdictional models of property control in India and the disruption of criminal infrastructures in Vietnam. This enabled an assessment of the effectiveness of transforming technical on-chain data into a legally significant evidentiary base and tangible law enforcement outcomes, identification of critical limitations of blockchain analytics (obfuscation methods, lack of off-chain artefacts), and formulation of directions for standardising expert reports to enhance the reproducibility and evidentiary robustness of conclusions in judicial proceedings, particularly in India and Vietnam. A limitation of the study was the use of exclusively open-source data concerning India and Vietnam, the uneven detail of available reports, and the probabilistic nature of analytical conclusions in blockchain forensics, particularly regarding attribution and the reconstruction of complex obfuscation schemes.

Results

Effectiveness of blockchain forensics in cybercrime investigations in India and Vietnam

Blockchain forensics (or cryptocurrency forensics) in the context of cyber investigations was a set of methods for collecting, normalising, analysing, and interpreting data from blockchain networks and associated digital artefacts with the aim of establishing facts regarding the movement of assets, relationships between addresses, and events relevant to criminal proceedings (Atlam *et al.*, 2024). In practice, blockchain forensics was predominantly applied by combining on-chain data with off-chain sources (data from exchanges/custodial services, wallet providers, devices, network logs, etc.), as the blockchain itself contains a limited set of attributes sufficient for the legal identification of a specific individual (Dudani *et al.*, 2023). The basic abstraction of analysis was the transaction graph, where nodes represent addresses/accounts and/or transactions, edges represent asset transfers between addresses, considering direction, time, and value. The graph representation allows for the reconstruction of asset movement sequences, identification of 'concentration nodes', identification of typical "layering" patterns, and determination of probable entry/exit points into the fiat system. In investigative practice, it was necessary to distinguish between an address as an identifier on the network (a public key or derived value depending on the blockchain) and a wallet as a software/hardware mechanism for managing keys and signing transactions. This distinction has implications for evidentiary value: the blockchain records addresses and transactions, while control over the wallet (keys) was established through devices, seed phrases, backups, or through the provider of custodial services (Dudani *et al.*, 2023, Atlam *et al.*, 2024).

One of the key approaches was address clustering, i.e., the grouping of addresses that were likely controlled by a single entity or belong to a single service infrastructure. Such conclusions were based on heuristics specific to a particular network and transaction model (for example, for Unspent Transaction Output (UTXO) networks – change address patterns), as well as on behavioural indicators (frequency, rhythm, typical routes) (Dudani *et al.*, 2023; Atlam *et al.*, 2024). Clustering was probabilistic in nature and requires documenting assumptions and verifications, as clustering errors can impact legal interpretation. A critical point for identification was the VASP – exchanges, bureaux de change, custodial providers. These entities may possess Know Your Customer (KYC)/AML data and operational logs linking blockchain addresses/accounts to real identities or payment instruments (Dudani *et al.*, 2023; Atlam *et al.*, 2024). In practical terms, this means that on-chain analysis was used to identify relevant addresses and transaction routes, after which interaction with VASPs within procedural frameworks becomes critical.

Blockchain forensics deals with reproducible artefacts that can be re-examined: transaction identifiers, transaction linkage to a block, timestamps (temporal context, which depends on the protocol/network and was not always a precise "real-time" marker of the event), as well as input/output addresses, amounts, fees, and smart contract call parameters (where applicable). Crucially, the data source (node, indexing provider, analytical tool) must be correctly recorded, and the "reproducibility" of the procedure for obtaining results must be ensured, as discrepancies in sources/indexing or tool parameters can affect interpretation (Dudani *et al.*, 2023; Atlam *et al.*, 2024). Given the probabilistic nature of clustering and the dependence of attribution on off-chain sources, it was advisable to correlate blockchain forensics results with typical criminal typologies and procedural requirements. In different scenarios, key roles may be played either by the gaps between on-chain transfers and off-chain platform data, or by the service infrastructure, conversion, and interaction with VASPs as sources of KYC/AML data. Simultaneously, the requirements of evidence remain immutable: recording the data source, describing tools and procedures, ensuring reproducibility of results, and maintaining the chain of custody for relevant digital artefacts (Table 1).

Table 1. Scenarios of crypto-asset use in cybercrime and requirements for procedurally admissible evidence

Scenario	Characteristics	Typical Limitations/ Countermeasures	Key Evidence Requirements
Investment scam / Ponzi, "crypto platforms"	On-chain routes (txid, addresses, token transfers), correlation with off-chain data, graph analysis/ clustering, "anchors" via VASPs	Off-chain balances may be falsified; amount splitting; use of different networks/routes; dependence on VASP data availability	Chain of custody for devices/logs; procedurally correct acquisition of off-chain data; transparency of methodology and minimisation of assumptions

Continued Table 1

Scenario	Characteristics	Typical Limitations/ Countermeasures	Key Evidence Requirements
Pseudo-exchanges / pseudo-DEXs (fraudulent "services")	Deposit addresses/conversion routes, intersections with VASPs, infrastructure analysis (domains/logs)	Cross-chain transfers; use of intermediaries; rapid infrastructure changes; imitation of DeFi functions without genuine decentralisation of control	Procedural seizure/preservation of digital traces (servers/logs/accounts); chain of custody; formalising requests to providers
Stablecoins (USDT) as a common payment pattern in crypto scenarios	Token transfers, on/off-ramps, attribution via VASPs, graph patterns	High velocity of movement; multi-chain nature of stablecoins; sum fragmentation; circumvention via intermediary services	AML mechanisms for requesting data/restricting transactions; documenting data sources and ensuring reproducibility
Ransomware (contextual scenario)	Payment patterns/tracing in Bitcoin; large-scale on-chain activity analysis Bitcoin	Use of trace obfuscation techniques; rapid movement and splitting; dependence on availability of off-chain data	Chain of custody for digital artefacts; reproducibility of on-chain pattern interpretation

Source: compiled by the author based on A.B. Turner *et al.* (2020), F.-C. Tsai (2021), S. Dudani *et al.* (2023), N.T. Nguyen *et al.* (2023), H.F. Atlam *et al.* (2024)

The effectiveness of investigations involving a crypto component was determined not merely by the fact of on-chain tracing, but by the presence of attribution points and the ability to transform technical findings into procedurally admissible evidence. On-chain analysis (graph, clustering, route reconstruction) primarily serves as "navigation", whereas the decisive stage was reaching off-chain sources – primarily VASPs and related Know Your Customer (KYC)/ AML data or service infrastructure artefacts. Hence, a key limitation follows: the more a criminal model avoids regulated services (cross-chain transfers, intermediaries, rapid infrastructure changes, obfuscation), the harder it was to transition from tracing to an evidentially complete outcome. Scenarios differ in the type of "gap" between on-chain and off-chain data: for Ponzi/pseudo-platforms, falsified internal balances were critical; for pseudo-exchanges, it was control over withdrawal points and infrastructure instability. Stablecoins represent more of a payment pattern, reinforcing the importance of rapidly identifying off-ramps and applying AML mechanisms. Common to all scenarios were the requirements of evidence – chain of custody, reproducibility of the methodology, and documentation of data sources and assumptions; without these, on-chain analysis remains an analytical, not a procedural, result.

The regulatory and legal framework determines how the state can qualify cybercriminal acts, obtain, secure, and evaluate digital evidence, and identify and restrict the movement of criminal proceeds, including assets in the form of cryptocurrencies. To assess the application of blockchain forensics in cybercrime investigation, the interaction of two domains was key: the cyber domain (incident, data, and infrastructure handling) and the financial-legal domain (AML, seizure/freezing/confiscation of assets). In practical terms, the former domain provides access to digital traces, while the latter creates the legal mechanism for implementing investigation results concerning assets and proceeds. The Act of the Information Technology No. 21 (2000) forms the basic framework for legal response to cyber incidents and legitimises work with digital artefacts (electronic data, computer systems, logs, communications, service data). Concurrently, in crypto cases, the Act serves as the "entry-level" legal layer: it supports the qualification of the cyber incident and work with digital traces, but does not provide a self-sufficient mechanism for legal control over crypto-assets as criminal proceeds. Therefore, in cases where cybercrime was monetised through crypto-assets, the financial-legal perspective becomes decisive. The central instrument in this domain was The Prevention of Money-Laundering Act No. 15 (2003), which allows property or the value of property derived from unlawful activity to be considered an object of special state measures. For crypto cases, this was critical: an on-chain asset (cryptocurrency/tokens) or funds converted into crypto can be placed under legal control as the equivalent of criminal proceeds. Blockchain forensics establishes transaction routes and points of intersection with services/wallets; however, practical effectiveness for the law enforcement system was achieved when the technical result was transformed into a procedural action (access restriction, freezing, seizure, prospect of confiscation).

Consequently, the indicator of success was not only the reconstruction of the transaction route but also the achievement of legal control over the asset through freezing or seizure. Institutionally, The Prevention of Money-Laundering Act No. 15 (2003) was implemented through the competencies of financial law enforcement agencies; for instance, public communications by the CoinDesk (2025) describe tracing complex transaction chains, identifying crypto-wallets, and the subsequent seizure/control of assets under The Prevention of Money-Laundering Act No. 15 (2003). For India, the effectiveness of blockchain forensics should be assessed through the link: "on-chain tracing → identification of a controlled point/vehicle → procedural action under The Prevention of Money-Laundering Act". Separately, the issue of the legal status of crypto-assets

must be considered. The Indian approach to crypto-assets also has a constitutional-legal dimension, which sets the boundaries for regulatory measures and law enforcement, providing the theoretical foundation explaining the multi-component nature of the regulatory model (combining cyber law, AML logic, and public law principles).

The Normative Model of Vietnam was described as three-layered. Law on Cybersecurity No. 24 (2018) establishes the framework for state response to cyber incidents and regulatory interaction in cyberspace, including the powers of relevant authorities and requirements for digital infrastructure entities. This law creates the environment for data access and incident response; without it, on-chain outcomes lack sufficient procedural support from off-chain artefacts (logs, accounts, communications) necessary for evidentiary purposes. Anti-Money Laundering Law No. 14 (2022) (effective from 01.03.2023) establishes the financial-legal basis for combating money laundering and international cooperation. Its applied significance lies in forming procedural grounds for financial control and the application of restrictive measures. The Criminal Procedure Code No. 101 (2015) defines the procedure for obtaining, securing, and evaluating evidence, and consequently, the conditions under which digital artefacts related to crypto-assets acquire procedurally admissible status. Analytically, this was key for assessing effectiveness: even high-quality on-chain analysis loses practical value without the procedurally correct acquisition and recording of off-chain data and the proper documentation of the chain of evidence.

In summary, India and Vietnam differ in the configuration of the legal "circuits" for converting on-chain analysis into a procedural outcome. In India, the cyber circuit (Act of the Information Technology No. 21, 2000) provides the legal basis for working with digital artefacts, while the financial-legal circuit (The Prevention of Money-Laundering Act of India No. 15, 2003) provides the instruments for property-related measures. Consequently, practical effectiveness was more frequently documented in the forms of freeze/seizure/attachment after gaining access to controlled infrastructure or key storage media. In Vietnam, the normative model was three-layered (cyber response – AML – criminal procedure), and the ultimate effect depends on the coordinated access to off-chain artefacts and their procedural documentation, which was critical in cases dominated by pseudo-platforms and "virtual" balances. The differences in the types of publicly documented outcomes between jurisdictions were explained not by the technical capabilities of on-chain analysis, but by the varying institutional and procedural capacity to rapidly integrate the cyber circuit with financial-legal mechanisms and evidentiary requirements.

The effectiveness of blockchain technology application in cyber investigations

For crypto cases, what was decisive was not merely "transaction identification", but evidential reliability, particularly an unbroken chain of custody. A technological approach discussed in the literature was the "blockchain of custody" – recording key events in the evidence lifecycle in an immutable ledger (Tsai, 2021). However, this does not substitute for procedural requirements concerning initial seizure and forensic handling and was only meaningful as an additional mechanism for integrity control. Separately, the practical effectiveness of blockchain analysis depends on the ability to trace an on-chain trail to a controlled/identifiable point (service/provider/infrastructure); typical barriers include obfuscation, the use of services that complicate tracing, rapid movement of assets between instruments/networks, and other techniques that increase the risk of clustering errors and dependence on off-chain data (Dudani *et al*., 2023; Atlam *et al*., 2024). A distinct class of problems was constituted by "off-chain" fraudulent schemes, where legally significant was the separation of simulated interface data from the actual on-chain movement of assets (Nguyen *et al*., 2023). Cross-country differences manifest in the method of legally converting the on-chain trail: in Indian cases, effectiveness was documented through procedurally formalised measures against assets, whereas in Vietnamese cases, it was through a combination of dismantling the scheme and the procedural documentation of evidence within the cyber framework, AML countermeasures, and criminal procedure. On this basis, Table 2 was presented, demonstrating how the respective legal circuits were implemented in the practice of India and Vietnam, from the type of offence and crypto-component to specific actions by authorities and measurable outcomes.

Table 2. Practical implementation of regulatory circuits in crypto cases in India and Vietnam

Country / Case	Type of Offence	Blockchain/Crypto Component	Actions by Authority	Outcome
India BitConnect, 15.02.2025	Crypto-investment fraud / "cryptocurrency fraud"	Analysis of "complex web of transactions" in crypto wallets, use of dark web to complicate tracing	Tracking/analysis of transaction network, searches, seizure of digital devices, seizure of crypto with transfer under ED control	Seizure of crypto assets ~ ₹1,646 crore (approx.), ₹13,50,500 in cash and a Lexus car, as well as digital devices; previously (within this case) property attached worth ~ ₹489 crore (approx.)
India E-Nuggets, 28.09.2022	Cyber fraud / money laundering	Exchange route (WazirX → Binance), BTC as object of freezin	Tracing the route, freezing BTC on Binance, searches (cash seizure)	77.62710139 BTC frozen, estimated equivalent: USD 1,573,466 (≈ ₹12.83 crore), cash of ₹17.32 crore seized earlier during search

Continued Table 2

Country / Case	Type of Offence	Blockchain/Crypto Component	Actions by Authority	Outcome
Vietnam, MTC / Matrix Chain, 28.05.2025	Investment fraud via "sàn giao dịch tiền ảo" (pseudo-platform)	Crypto platform as a mechanism for raising funds, focus on scale of fundraising / investments/ losses: "gần 10 ngàn tỷ đồng" (nearly 10 trillion VND) (software development cost 20,000 USDT, "platform" model specified: each participant pays 1 USDT into a "platform fee wallet", stated proportions of fund distribution from "platform fee wallet": 40% / 5% / 55% (leaders/advertising/ personal use)	Operational measures/ operation, uncovering the scheme	Scale: "gần 10 ngàn tỷ đồng", cited 394,276,762 USDT (~ over 10,000 billion VND) and >138,000 accounts
Vietnam, KAYPLE, 21.12.2025	Fraud involving investor solicitation	as a payment crypto-layer, funds transferred to crypto wallets controlled by the organiser; "balances" in the interface described as "virtual"	Uncovering; procedural actions against involved persons, establishing the scale of damage	Scale of damage (crypto + equivalent) – number of investor "wallets": over 4,000; amount linked to crypto payments: over 51 million USDT, equivalent in national currency ~ 1.275 billion VND (1.275 trillion VND); procedural outcomes (detentions/expansion) – apart from the two main figures, the release notes the detention of another 8 related individuals (+8 total)
Vietnam, Winrich/Wintop, 30.12.2021	Fraud via web platforms	Route: purchase on an exchange (Binance mentioned) ➔ conversion to USDT ➔ transfer to organisers wallet	Uncovering; detention of involved persons, recording victim statements	At the time of the release publication, there were already 9 statements, and the total amount of misappropriated funds according to these statements exceeded 12 billion VND

Source: compiled by the author based on Ho Chi Minh City Public Security Department (2021), India Today (2022), CoinDesk (2025), Ministry of Public Security (2025a), Ministry of Public Security (2025b)

The application of blockchain technologies in the investigation of cybercrimes proves effective not as a self-sufficient evidentiary tool, but rather as a navigational and analytical layer. This layer enables the restoration of fund flows, the identification of controlled "points of influence" (primarily VASPs/exchanges, custodians, devices, and accounts), and the subsequent conversion of on-chain findings into procedural actions. An analysis of publicly documented outcomes reveals distinct models for the "conclusion" of investigations. In the Indian cases, the emphasis was placed on property-related measures with quantifiable volumes (freeze/seizure/attachment). This reflects a focus on the financial and legal control of assets and the swift achievement of tangible property results through regulated infrastructure or physical access to storage media/keys. This was evident, for instance, in the E-Nuggets case, where tracing the exchange route creates a point of control for freezing BTC, and also in the BitConnect case, where, despite tracing difficulties, the outcome was achieved by combining on-chain tracing with searches and the seizure of digital devices and crypto assets. In contrast, the Vietnamese cases typically involve large-scale investment frauds with a pronounced "off-chain" component (pseudo-platforms, "virtual" balances in user interfaces, organisational networks for soliciting investments). Here, the blockchain primarily serves as a payment layer and an indicator of scale, with publicly documented effectiveness manifested through the exposure and dismantling of schemes, arrests, and the documentation of the scale of funds or accounts involved. In such models, the evidentiary "stitching" together of on-chain payments with off-chain artefacts (accounts, platform logs, communications, KYC/AML data) becomes critical. Without this, on-chain conclusions remain technically plausible but procedurally vulnerable. Overall, the difference between India and Vietnam within the examined cases was explained not so much by the analytical tools employed, but by the availability of attribution control points and off-ramp infrastructure, the specific weight of the off-chain component in the criminal modus operandi, and the capacity of the legal framework to promptly transform technical findings into tangible property and procedural outcomes. This ultimately determines the measurable effectiveness of blockchain forensics in investigative practice.

The evaluation of the effectiveness of applying blockchain technologies in cybercrime investigations was conducted on the basis of operationalised metrics that reflect the stages of transforming a technical trace (on-chain data) into a law enforcement outcome. The proposed metrics align with approaches described in the literature on

cryptocurrency/blockchain forensics and the admissibility of digital evidence (Tsai, 2021; Dudani *et al.*, 2023; Atlam *et al.*, 2024). Given the uneven level of detail in official press releases, the assessment was conducted according to the principle of "publicly documented / not documented", without reconstructing missing procedural details. Key metrics include: Asset restraint / recovery – whether the freezing, seizure, or other legal restraint of assets (including crypto assets) was documented, and whether volumes/amounts were specified; Disruption – whether the termination of the scheme/platform, arrests, searches, or other measures that prevent the continuation of the offence were documented; Attribution leverage – whether "bridges" between on-chain data and specific individuals/organisations (VASPs/exchanges, wallet control, seized devices, account credentials) were documented; Evidentiary robustness – whether approaches to preserving/documenting digital evidence (chain of custody, seizure of storage media, handling of keys, etc.) were described; in their absence, this aspect was assessed as "not documented", with standards substantiated by scientific literature; Time-to-intervention – whether the source contains temporal markers allowing for an assessment of the interval between the event/discovery and key measures; in the absence of a chronology – "not documented". The structural and logical model of the operational chain for transforming on-chain data into a law enforcement outcome was presented in Figure 1.

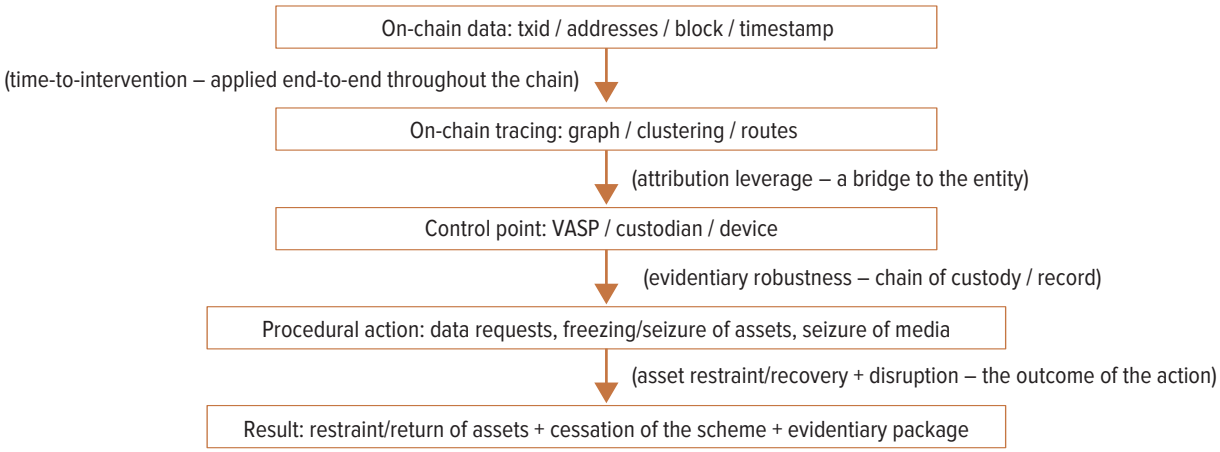

Figure 1. Structural and logical model of the operational chain for transforming on-chain data into a law enforcement outcome

Note: time-to-intervention was a cross-cutting metric for the entire chain, while evidentiary robustness was assessed based on procedural formalisation and chain of custody at the stage of procedural actions

Source: compiled by the author based on F.-C. Tsai (2021), S. Dudani *et al.* (2023), H.F. Atlam *et al.* (2024)

To assess effectiveness, it was advisable to consider not only on-chain analysis tools but also the operational chain of law enforcement actions: recording the initial report and collecting digital artefacts (addresses, TXIDs, communications); conducting on-chain analysis and identifying entry/exit points; identifying intermediary services (exchanges/VASPs); undertaking procedural actions to preserve data and restrict asset disposition; liaising with foreign jurisdictions; and formalising evidence in accordance with criminal procedure requirements. The presence of AML mechanisms and procedural protocols was decisive for the transition from technical tracing to property measures and proof in criminal proceedings. The synthesis presented in Table 2 indicates differences in the type of publicly documented outcomes: in the Indian cases, the emphasis was on property measures (freezing, seizure, attachment of assets) with quantifiable amounts, whereas in the Vietnamese cases, the focus was on exposing schemes, making arrests, and highlighting the scale of funds involved; information on the freezing or seizure of crypto assets was presented much more sparingly in public communications.

In India, on-chain tracing combined with the seizure of digital storage media predominantly yields results in the sphere of financial and legal asset control, reflected in indicators of freezing/seizure. The rapid transition from the on-chain graph to attribution points through regulated intermediaries (VASPs) and subsequent procedural actions was decisive. However, limitations include obfuscation techniques, cross-chain transfers, and the circumvention of regulated infrastructure, which complicate proving ownership and recovering assets. The Vietnamese cases typically involve large-scale investment frauds with a significant "off-chain" component, where the on-chain data serves as a payment channel and an indicator of scale. Effectiveness here was demonstrated through the dismantling of schemes and the documentation of the scale and network of involved entities, rather than solely through property-related outcomes. The main risks were associated with a deficit of off-chain data and its short retention periods, the multi-network nature of stablecoins, and manipulations with off-chain balances. To ensure evidentiary robustness, clear procedures

concerning data sources, reproducibility, and the chain of custody were necessary; otherwise, on-chain conclusions remain technically plausible but procedurally vulnerable.

Therefore, it was advisable to formulate directions for practical recommendations aimed at standardising working procedures, enhancing reproducibility, and minimising the loss of evidentiary information at the "on-chain ↔ off-chain" interface. It was necessary to formalise a typical sequence of actions: "on-chain tracing → establishing a point of control (VASP/custodian/device) → procedural action" (data request, freezing/seizure of assets, seizure of storage media). To unify outcomes in each case, it was recommended to document a minimum set of technical artefacts: txid, addresses, block height, temporal markers, as well as relevant parameters of token transfers/smart contracts (where applicable). Separate chain of custody rules should be established for hardware and mobile wallets, seed phrases, private keys, backups, and account access credentials. Mandatory elements must include access logging, integrity controls (hashing), role-based access segregation, and regulated conditions for the storage and transfer of storage media/data between units.

To enhance the evidentiary resilience of conclusions, it was advisable to systematically combine on-chain analytics (transaction graphs, clustering, typical transaction routes) with off-chain sources: KYC/AML data from VASPs, platform logs, and telecommunications and payment trails. This approach reduces reliance on probabilistic heuristics and increases the reproducibility of attribution claims. Given that relevant data (log records, account information, technical metadata) may have limited retention periods, and assets move rapidly between networks and services, it was prudent to formalise channels for expedited inquiries to VASPs and procedures for mutual legal assistance. This increases the likelihood of the timely application of restrictive measures and the preservation of evidence. It was recommended to unify the report structure for blockchain forensics, mandating a description of: the methodology, data sources (node/indexer provider), tools and their parameters, assumptions and verifications, as well as the steps necessary for result reproduction. This reduces the risk of methodological discrepancies and simplifies expert evaluation and judicial verification. It was advisable to include practical modules in training programmes on blockchain forensics, the typology of crypto-fraud (investment schemes, pseudo-platforms, stablecoin usage), interaction with exchange/custodial infrastructure, as well as the basic principles of evidentiary assessment of digital artefacts and the requirements for the procedural documentation of results. Thus, the effectiveness of employing blockchain forensics in cybercrime investigation was determined not by on-chain tracing itself, but by the presence of controlled attribution points (primarily VASPs) and the capacity of the legal framework to convert technical findings into procedural actions concerning assets and evidence.

Discussion

The study's results demonstrated that the effectiveness of applying blockchain forensics depends not solely on technical tracing, but on the complete implementation of the operational chain for transforming data into admissible evidence. This aligns with the findings of A. Trozze *et al.* (2022), who, in their systematic review, harmonise the definition of crypto-frauds and incorporate practitioner assessments (expert consensus), thereby strengthening the "bridge" between academic models and law enforcement/regulatory reality. This directly corresponds to the approach in the current study of "publicly documented/not documented" and to the fact that different jurisdictions publish different types of outcomes: in India – predominantly freeze/seizure/attachment with volumes, in Vietnam – disruption and the scale of involvement. Furthermore, the work of G. Arnone *et al.* (2025) demonstrates the mechanisms by which organised groups use cryptocurrencies for money laundering, fraud, and extortion, while also highlighting the gaps/limitations of enforcement frameworks and the need for cross-border cooperation. This correlates with the assertion of the current study that the presence of AML mechanisms and procedural frameworks was decisive for the transition from technical tracing to asset-related measures and proof. This precisely explains the differences in the types of publicly documented outcomes between jurisdictions and the varying conversion of on-chain analytics into asset seizure/forfeiture or scheme disruption.

The studies by B. Acharya & T. Holz (2024) and S. Ji *et al.* (2023) approach the problem differently, yet demonstrate a common conclusion: in contemporary 21st-century crypto-frauds, technical on-chain analysis was necessary but predominantly insufficient for achieving a law enforcement outcome. In the case of "pig butchering" demonstrated by B. Acharya & T. Holz (2024), off-chain communications, fake investment infrastructure, and social engineering play a key role, whereas the blockchain was used primarily as a payment channel. In contrast, S. Ji *et al.* (2023) found that even with advanced methods for detecting scam patterns (including Machine Learning (ML) approaches), the primary practical barrier remains the conversion of detected on-chain indicators into subject attribution, procedural actions, and an evidentiary base. This correlates with the results of the current study, where effectiveness was determined by the ability to integrate on-chain traces with off-chain data and infrastructural control points (VASPs, accounts, devices, user accounts), as evidenced in the KAYPLE case involving "virtual balances" and real payments in USDT to controlled wallets. The real effectiveness of blockchain forensics was determined not merely by the detection of on-chain patterns, but primarily by their procedural verification through off-chain sources and points of infrastructural control, which ensures attribution and the transformation of technical data into admissible evidence and effective measures of influence.

The study's results indicated that a key condition for converting on-chain analysis into practical outcomes was

the rapid transition to attribution points through regulated intermediaries (VASPs) and subsequent procedural actions for data preservation and asset restraint, which aligns with the conclusions of A.B. Turner *et al.* (2020). The authors synthesised analysis techniques for illicit Bitcoin transactions and emphasised that attribution in a pseudonymous environment remains the key barrier. Practically significant outcomes require the combination of blockchain analytics with legal and organisational response mechanisms. Tracing was merely one stage, while the outcome was shaped through procedural actions and interaction with infrastructure providers. Illustrative in this context was the E-Nuggets case, where the documented outcome was linked to reaching exchange infrastructure and freezing BTC, i.e., the realisation of a "control point".

In their work, C. Carpentier-Desjardins *et al.* (2025) identified an evidence-based taxonomy of Decentralized Finance (DeFi) crime and demonstrated the role of DeFi actors as targets, intermediaries, or even malicious participants. The authors operationalise the role of DeFi actors in events as targets, intermediaries, or malicious participants, demonstrating that criminal activity can be directed against legitimate protocols as well as realised through maliciously created infrastructure. Empirical results show that events where DeFi actors were targets constitute approximately half of the incidents but were associated with the dominant share of aggregate financial losses, whereas events initiated by DeFi actors as perpetrators account for a smaller share of losses. Furthermore, events were mapped to the technical layers of the DeFi stack, allowing differentiation between the levels where incidents concentrate and the levels where the greatest losses occur, with a notable role for the protocol and interface/oracle layers. These findings were consistent with the results of the current study regarding the limitations of purely on-chain detection without the rapid involvement of infrastructural control points and off-chain sources necessary for attribution and the procedural conversion of technical indicators into law enforcement outcomes. Metrics of disruption and attribution leverage become critical precisely for DeFi/pseudo-platforms, where detection without rapid access to a control point does not translate into a law enforcement outcome.

K.E. Castro Severiche *et al.* (2025) formulate research questions, specifically concerning publication trends, the classes/types of ML algorithms applied for model training, and the limitations and challenges of automated Ponzi scheme detection in decentralised transaction environments. The authors concluded that dominant solutions rely on features of transaction behaviour and/or smart contract characteristics, but their practical applicability was limited by issues of label quality, experiment reproducibility, and data and tool variability. This correlates with the current study's emphasis on formalised procedures, a standardised sequence of actions "on-chain → control point (VASP/custodian/device) → procedural action", and measuring effectiveness through operationalised metrics. This substantiates the need for standardising procedures for the reproduction of results concerning the mandatory description of tools and analysis parameters.

The research findings confirmed that on-chain analysis/graph techniques (including ML detection) serve as a form of "navigation", whereas reaching points of attribution/control and corroborating conclusions with off-chain data become decisive. In the absence of such points and off-chain verification, technical conclusions were difficult to transform into procedurally admissible evidence. This aligns with the work of H. Kanezashi *et al.* (2022), who demonstrated that heterogeneous Graph Neural Networks (GNNs) can enhance the quality of fraud/phishing detection in Ethereum by accounting for heterogeneous nodes and links, as well as issues of label imbalance. However, such approaches primarily facilitate the identification of suspicious patterns and probabilistic classification of activity, but they do not ensure subject attribution or the procedural admissibility of the obtained conclusions without involving off-chain sources and evidence preservation procedures. ML enhances the analytical stage, but the ultimate effect depends on integration with law enforcement procedures.

The research results indicated that the practical effectiveness of forensics with a crypto component depends on the completeness of the operational chain, specifically on the seizure/preservation of digital artefacts and the subsequent procedural conversion of the findings. In publicly documented cases, this was manifested through the combination of on-chain analysis with actions concerning devices and media (for example, the seizure of digital devices in the BitConnect case). This correlates with the approach of A. Bhattarai *et al.* (2025), as the authors propose instrumental automation precisely for the stage identified as critical in the current study – the rapid extraction and initial preservation of mobile digital artefacts necessary for subsequent procedural interpretation and attribution. In their study, A. Bhattarai *et al.* (2025) proposed a comprehensive approach to automating crypto-forensics on mobile platforms, combining ML, image processing, and Natural Language Processing (NLP) for the rapid automated extraction/triage of crypto-artefacts from Android and Apple mobile operating systems (iOS). The authors describe the automated detection of cryptocurrency wallets and associated artefacts (including logs/databases) on a device, as well as the extraction of relevant traces from images, web activity, and SMS communications. Procedurally correct handling of mobile wallets/keys and standardisation of the chain of custody for the relevant media and access credentials were essential.

In the work by Sakshi *et al.* (2023), a blockchain-oriented framework, the Blockchain-based Evidence Preservation Framework for Internet of Things (BEvPF-IoT), was proposed for preserving multimedia digital evidence from IoT environments to ensure its integrity and traceability. The solution combines Ethereum as a register for metadata/hashes and the InterPlanetary File System (IPFS) as a distributed content store, allowing the separation of large file storage from their immutable logging. The authors defined

a sequence of forensic processing operations (registration, storage, access/verification) aimed at minimising the risks of unauthorised modification of evidence. The feasibility of the approach was substantiated experimentally through performance evaluation and overhead assessment in the blockchain network (including latencies and operational costs). This correlates with the evidentiary robustness metric in the current study, where effectiveness was evaluated based on the presence of a documented chain of custody and the procedural admissibility of digital evidence. At the same time, the results of this study underscored that blockchain-based registration mechanisms cannot replace primary seizure and forensic preservation; instead, they serve a supplementary function of confirming immutability and access control after evidentiary materials have been obtained. Effectiveness, as understood in the current study, was determined by the integration of such registration mechanisms into the full operational chain and adherence to chain of custody procedures. Thus, the differing institutional capacities of jurisdictions to implement the operational forensic chain leads to variations in publicly documented outcomes (freeze/seizure/attachment or disruption). Therefore, enhancing practical effectiveness requires not only the development of detection methods but, above all, the strengthening of procedural and infrastructural mechanisms that ensure attribution and the procedural transformation of on-chain indicators into legally significant evidence and coercive measures.

Conclusions

The research outcomes defined blockchain forensics as a set of methods for collecting, normalising, and analysing data from blockchain networks to establish links between addresses and events relevant to criminal proceedings. The fundamental analytical model was the transaction graph, which reflects the movement of assets considering time and amount, enabling the identification of concentration nodes, layering schemes, and points of entry/exit into the fiat system. In the context of proving facts, a distinction must be made between the address as a network identifier and the wallet as a key management mechanism; actual control over assets was confirmed through access to seed phrases, private keys, or custodial services. Since address clustering was probabilistic in nature, the results necessitate mandatory documentation of assumptions to avoid errors in legal interpretation. Intermediaries (VASPs) possess critical operational logs that link blockchain accounts with real-world payment instruments. To ensure the reproducibility of an investigation, the precise set of technical artefacts must be recorded: txid, block height, timestamps, and smart contract call parameters. Stablecoins were considered a prevalent payment pattern, requiring the rapid identification of off-ramp points for the application of AML procedures. The effectiveness of an investigation was based on the interaction between the cyber domain (infrastructure-focused work) and the financial-legal domain (asset seizure mechanisms).

Vietnams regulatory model operates on three levels: cyber incident response, financial anti-money laundering measures, and the criminal procedural evaluation of evidence. In the Matrix Chain case (Vietnam), the use of a "platform fee wallet", to which each participant paid a fixed fee of 1 USDT, was documented. An additional mechanism for controlling the integrity of the evidence lifecycle was the blockchain of custody approach, which complements rather than replaces the primary seizure of artefacts. In the Indian BitConnect case, besides the seizure of digital devices, the confiscation of a Lexus car and over 1.3 million Indian rupees in cash was documented, alongside the attachment of ancillary property valued at 4.89 billion rupees. Furthermore, in the E-Nuggets case, tracing the exchange route WazirX → Binance enabled the freezing of cryptocurrency and the additional seizure of cash amounts totalling 173.2 million rupees during searches. A difference in case resolution models was observable between the countries: in India, asset-related measures dominate due to rapid access to regulated infrastructure or physical access to keys. In Vietnam, large-scale investment frauds with an off-chain component (pseudo-platforms, "virtual" balances) were more prevalent, where the blockchain serves as a payment layer, and the outcome was primarily recorded as the disruption of schemes and the arrest of organisers. Ultimately, effectiveness in both jurisdictions was determined by the ability to promptly convert tracing into procedural actions against assets and individuals. It was advisable to unify the structure of expert reports, including a description of data indexing sources and the steps necessary to reproduce the analysis results. Future research should be directed towards standardising the interaction of law enforcement agencies with VASPs, automating the analysis of DeFi and cross-chain operations, and utilising ML for the preventive detection of fraudulent patterns under conditions of high obfuscation.

Acknowledgements

None.

Funding

None.

Author Contributions

Aigerim Shegebaeva established the methodological framework for research into blockchain forensics and developed a set of criteria for assessing its effectiveness in the investigation of cybercrimes. The author analysed the legal frameworks of India and Vietnam, examined practical case studies involving BitConnect, E-Nuggets, Matrix Chain, KAYPLE and Winrich/Wintop, and formulated recommendations regarding the standardisation of work with on-chain data, VASPs, digital artefacts and evidence.

Conflict of Interest

None.

References

[1] Acharya, B., & Holz, T. (2024). An explorative study of pig butchering scams. *ArXiv*. doi: 10.48550/arXiv.2412.15423.

[2] Act of the Information Technology No. 21. (2000, June). Retrieved from https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

[3] Anti-Money Laundering Law No. 14/2022/QH15. (2022, November). Retrieved from https://vanban.chinhphu.vn/?classid=1&docid=207710&pageid=27160&typegroupid=.

[4] Arnone, G., Scire', G., & Bivona, E. (2025). The (mis)use of cryptocurrencies by criminal organizations: A systematic literature review. *Digital Finance*, 7, 815-851. doi: 10.1007/s42521-025-00148-1.

[5] Atlam, H.F., Ekuri, N., Azad, M.A., & Lallie, H.S. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. *Electronics*, 13(17), article number 3568. doi: 10.3390/electronics13173568.

[6] Bhattarai, A., Sahin, A., Veksler, M., Kurt, A., Aras, D., Imery, C., & Akkaya, K. (2025). Cryptocurrency forensics automation: A deep learning and NLP-based approach for mobile platforms. *Discover Computing*, 28, article number 123. doi: 10.1007/s10791-025-09595-1.

[7] Carpentier-Desjardins, C., Paquet-Clouston, M., Kitzler, S., & Haslhofer, B. (2025). Mapping the DeFi crime landscape: An evidence-based picture. *Journal of Cybersecurity*, 11(1), article number tyae029. doi: 10.1093/cybsec/tyae029.

[8] Castro Severiche, K.E., Wahlqvist Odenman, A., & Jalali, A. (2025). Ponzi scheme detection and prevention in blockchain platforms using machine learning: A systematic literature review. In P. Delir Haghighi, M. Greguš, G. Kotsis & I. Khalil (Eds.), *Information integration and web intelligence. Lecture notes in computer science* (Vol. 15342, pp. 87-102). Cham: Springer. doi: 10.1007/978-3-031-78090-5_8.

[9] CoinDesk. (2025). Retrieved from https://surl.li/qtjesk.

[10] Criminal Procedure Code No. 101/2015/QH13. (2015, November). Retrieved from https://vanban.chinhphu.vn/default.aspx?docid=183217&pageid=27160.

[11] Dudani, S., Baggili, I., Raymond, D., & Marchany, R. (2023). The current state of cryptocurrency forensics. *Forensic Science International: Digital Investigation*, 46, article number 301576. doi: 10.1016/j.fsidi.2023.301576.

[12] Ghosh, K., & Das, P.K. (2025). Comprehensive analysis of cryptocurrency, virtual digital assets, and distributed ledger technology with insights into Indian policies and research trends. *Discover Analytics*, 3, article number 3. doi: 10.1007/s44257-025-00030-9.

[13] Halder, D., & Saiyed, A.A. (2022). Legal challenges to cryptocurrency and its guardian-less victims in India: A critical victimological analysis. *International Annals of Criminology*, 60(1), 79-98. doi: 10.1017/cri.2022.6.

[14] Ho Chi Minh City Public Security Department. (2021). Retrieved from https://congan.hochiminhcity.gov.vn/wps/portal/Home/trang-chu/noi-dung-chi-tiet/tin-chuyen-nganh/tin%20hoat%20dong/catp%20triet%20pha%20san%20giao%20dich%20tien%20ao%20lua%20dao.

[15] India Today. (2022). Retrieved from https://www.indiatoday.in/india/story/ed-freezes-crypto-assets-worth-crores-e-nuggets-mobile-app-case-2005876-2022-09-28.

[16] Ji, S., Huang, C., Chu, H., Wang, X., Dong, H., & Zhang, P. (2024). Blockchain scam detection: State-of-the-art, challenges, and future directions. In J. Chen, B. Wen & T. Chen (Eds.), *Blockchain and trustworthy systems. BlockSys 2023. Communications in computer and information science* (Vol. 1896, pp. 3-18). Singapore: Springer. doi: 10.1007/978-981-99-8101-4_1.

[17] Kanezashi, H., Suzumura, T., Liu, X., & Hirofuchi, T. (2022). Ethereum fraud detection with heterogeneous graph neural networks. *ArXiv*. doi: 10.48550/arXiv.2203.12363.

[18] Law on Cybersecurity No. 24/2018/QH14. (2018, June). Retrieved from https://vanban.chinhphu.vn/?docid=206114&pageid=27160.

[19] Luong, H.T., & Ngo, H.M. (2024). Understanding the nature of the transnational scam-related fraud: Challenges and solutions from Vietnam's perspective. *Laws*, 13(6), article number 70. doi: 10.3390/laws13060070.

[20] Ministry of Public Security. (2025a). Retrieved from https://mps.gov.vn/bai-viet/bat-khan-cap-nhom-doi-tuong-lap-san-giao-dich-tien-ao-loi-keo-nguoi-choi-voi-so-tien-dau-tu-gan-10-ngan-ty-dong-d22-t45318.

[21] Ministry of Public Security. (2025b). Retrieved from https://mps.gov.vn/bai-viet/cong-an-dak-lak-triet-xoa-duong-day-lua-dao-1-275-ty-dong-1766313157.

[22] Nguyen, N.T., Nguyen, A.T., To, H.T.N., & Le, T.T.H. (2023). Why were Vietnamese people susceptible to cryptocurrency Ponzi schemes? Findings from using the PLS-SEM approach. *Journal of Financial Crime*, 31(1), 158-173. doi: 10.1108/JFC-12-2022-0299.

[23] Nguyen, T.T.T. (2025). Digital evidence in criminal procedure: Legal challenges and solutions in Vietnam. *Binh Duong University Journal of Science and Technology*, 8(1). doi: 10.56097/binhduonguniversityjournalofscienceandtechnology.v8i1.297.

[24] Prakash, F., & Sadawarti, H. (2022). Blockchain-based chain of custody: A secure digital evidence framework for digital forensics investigation. *Applied Innovative Research*, 3(1-4), 108-112.

[25] Sakshi, Malik, A., & Sharma, A.K. (2023). Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things. *Journal of Information Security and Applications*, 77, article number 103579. doi: 10.1016/j.jisa.2023.103579.
[26] Saniyazova, Y., Mediyev, R., Saitova, E., Utegenova, G., & Kzylkhojayeva, A. (2024). Advancing forensic science in Kazakhstan: The emergence and impact of digital forensics in cybercrime investigation. *Law, State and Telecommunications Review*, 16(2), 48-68. doi: 10.26512/lstr.v16i2.49190.
[27] Seerwani, P., & Ram Mohan, M.P. (2025). Virtual digital assets service providers under Indian insolvency framework (Working Paper No. 2025-10-01). Ahmedabad: Indian Institute of Management Ahmedabad.
[28] Shaisultanov, S., Akimzhanov, T., Abdrakhmanov, B., Bazarlinova, A., & Bazarlinova, A. (2024). Combating internet fraud through operative-search measures. *Law, State and Telecommunications Review*, 16(2), 257-275. doi: 10.26512/lstr.v16i2.50740.
[29] Simbayev, T. (2025). Legal issues of non-conviction-based confiscation of digital assets obtained through criminal means. *Law Journal*, 3(3), 88-114. doi: 10.47344/cmay9446.
[30] The Prevention of Money-Laundering Act No. 15. (2003, January). Retrieved from https://www.indiacode.nic.in/handle/123456789/2036?sam_handle=123456789%2F1362.
[31] Trozze, A., Kamps, J., Akartuna, E.A., Hetzel, F.J., Kleinberg, B., Davies, T., & Johnson, S.D. (2022). Cryptocurrencies and future financial crime: A systematic review. *Crime Science*, 11(1), article number 1. doi: 10.1186/s40163-021-00163-8.
[32] Tsai, F.-C. (2021). The application of blockchain of custody in criminal investigation process. *Procedia Computer Science*, 192, 2779-2788. doi: 10.1016/j.procs.2021.09.048.
[33] Turner, A.B., McCombie, S., & Uhlmann, A.J. (2020). Discerning payment patterns in Bitcoin from ransomware attacks. *Journal of Money Laundering Control*, 23(3), 545-589. doi: 10.1108/JMLC-02-2020-0012.