Information Dynamics and Applications
https://www.acadlore.com/journals/IDA

Cryptocurrency Investigations in Digital Forensics: Contemporary Challenges and Methodological Advances

Syed Atir Raza[1*], Mehwish Shaikh[2], Khadija Tahira[1]

[1] School of Information Technology, Minhaj University, 54000 Lahore, Pakistan
[2] Department of Software Engineering, Mehran University of Engineering and Technology, 76060 Jamshoro, Pakistan

[*] Correspondence: Syed Atir Raza (atirrazasyed@gmail.com)

Received: 07-25-2023 **Revised:** 08-02-2023 **Accepted:** 08-09-2023

Citation: S. A. Raza, M. Shaikh and K. Tahira, "Cryptocurrency investigations in digital forensics: Contemporary challenges and methodological advances," *Inf. Dyn. Appl.*, vol. 2, no. 3, pp. 126–134, 2023. https://doi.org/10.56578/ida020302.

Abstract: Digital forensics, a crucial subset of cybersecurity, encompasses sophisticated tools and methodologies for the interpretation, analysis, and investigation of digital evidence, facilitating the identification and mitigation of cybercrimes and security breaches. With the advent of cryptocurrencies, an array of unique challenges has emerged in the domain of digital forensic investigations. This review elucidates the prevailing state of digital forensic practices vis-à-vis cryptocurrencies, emphasizing the obstacles and limitations inherent in probing decentralized and intricate technologies. Notable deficiencies in extant investigative practices were observed. Solutions proffered encompass the formulation of novel software applications tailored for cryptocurrency analyses, the integration of machine learning and artificial intelligence capabilities, and the employment of advanced analytics to discern patterns and irregularities within blockchain transactions. Furthermore, a pioneering methodology, merging traditional digital forensic strategies with blockchain-specific techniques, is posited for efficacious cryptocurrency inquiries. The analysis underscores the imperative for a renewed paradigm in digital forensic examinations to surmount the challenges integral to cryptocurrency probes. By forging novel methodologies and standardizing investigative procedures, support for legal enforcement endeavors can be enhanced, facilitating the efficacious detection and prosecution of cryptocurrency-associated misdemeanors.

Keywords: Blockchain forensics; Digital forensics; Machine learning; Artificial intelligence; Challenges; Solutions

1 Introduction

Digital forensics, recognized as a pivotal facet of law enforcement and investigation, pertains to the collection, analysis, and preservation of digital evidence in support of legal proceedings [1, 2]. In recent times, a surge in the utilization of digital technologies has rendered digital forensics of paramount importance. Concurrently, cryptocurrencies, characterized as digital or virtual currencies that harness cryptography for security and operate without the oversight of central banks, have witnessed a meteoric rise in popularity. Such currencies, including but not limited to Bitcoin, Ethereum, and Litecoin, have unfortunately been appropriated for illicit activities ranging from money laundering and fraud to ransomware attacks. This has propelled the investigation of cryptocurrencies to the forefront of digital forensics disciplines [3–5].

The necessity to probe cryptocurrencies for digital evidence has been underscored by its role in thwarting unlawful endeavors [6]. Despite the allure of anonymity that cryptocurrencies extend to malefactors, the decentralized blueprint upon which they operate mandates the recording of every transaction on a publicly accessible ledger: the blockchain [7]. Enter the realm of blockchain forensics—a nascent discipline equipped with intricate tools and methodologies designed to sift through and analyze blockchain transactions, the blockchain structure is shown in Figure 1. This discipline facilitates the exposure of felonious activities, including money laundering and fraud, championing transparency and accountability in decentralized systems. Through the judicious application of the appropriate tools and techniques, it has been demonstrated that transactions can be retraced and culprits implicated within the blockchain's labyrinth [8, 9].

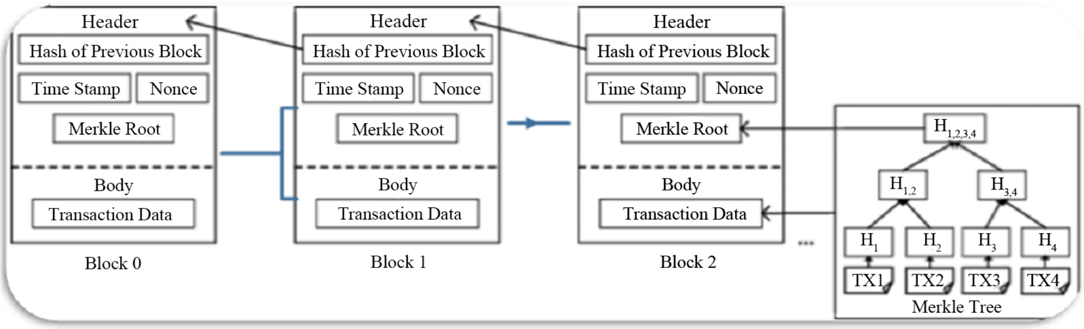

Figure 1. Blockchain structure

However, the task of decrypting cryptocurrencies for digital evidence is not devoid of formidable challenges. The independence that cryptocurrencies enjoy from central banking institutions and regulatory bodies complicates the execution of regulations and the pinpointing of wrongdoers [10]. Moreover, the dynamic landscape of cryptocurrencies, punctuated by the incessant introduction of novel currencies and technologies, poses a conundrum for digital forensics experts striving to remain updated with progressive techniques and instruments [11, 12]. As the appeal of cryptocurrencies continues to swell, it is anticipated that their appropriation for nefarious activities will follow suit. Encrypted files held for ransom by malefactors employing ransomware, and subsequent demands for payment in cryptocurrencies, further obfuscate the task of tracing fund movements and identifying culprits [13, 14]. The understanding of cryptocurrency transaction flow is crucial in decrypting these transactions and following the money trail to apprehend the perpetrators (Figure 2). Likewise, darknet markets, notorious for peddling unlawful goods and services, have showcased a penchant for cryptocurrencies as the favored transaction medium, ostensibly due to the veil of anonymity they proffer.

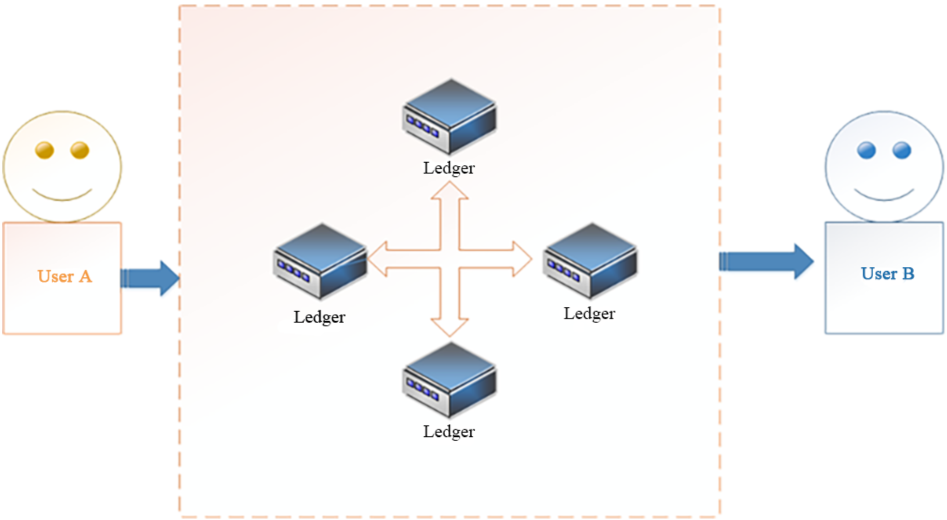

Figure 2. Cryptocurrency transaction flow

Given the aforementioned challenges, it remains imperative for experts in digital forensics to maintain cognizance of evolving developments in the cryptocurrency domain. The subsequent sections delve into the predominant issues and challenges intrinsic to the investigation of cryptocurrencies and elucidate potential solutions gleaned from the extant literature.

2 Related Works

The rise in the popularity of cryptocurrencies, recognized for their convenience in transactions and wealth storage, has inadvertently prompted a surge in their illicit usage. Consequently, a profound necessity has emerged for digital forensics to delve into crimes leveraging these currencies. Owing to the decentralized architecture of blockchain technology and the anonymity potentially granted by cryptocurrencies, novel challenges have been introduced to the domain of digital forensics [15, 16]. In light of these complexities, digital forensic methodologies have undergone considerable adaptation, seeking to navigate this altered landscape of digital evidence extraction.

Recent years have witnessed an influx of research in the realm of cryptocurrency forensics. Foremost among the areas explored has been the conception of forensic instruments and methods to scrutinize blockchain transactions [15, 16]. Through these innovative tools, investigators have been empowered to trace fund trajectories from one digital wallet to another, thereby discerning patterns indicative of suspicious undertakings. Such tools have been employed effectively in the elucidation of crimes encompassing money laundering, fraud, and the financing of terrorism [16]. As shown in Figure 3, it explains in detail how the blockchain is used for evidence investigation.

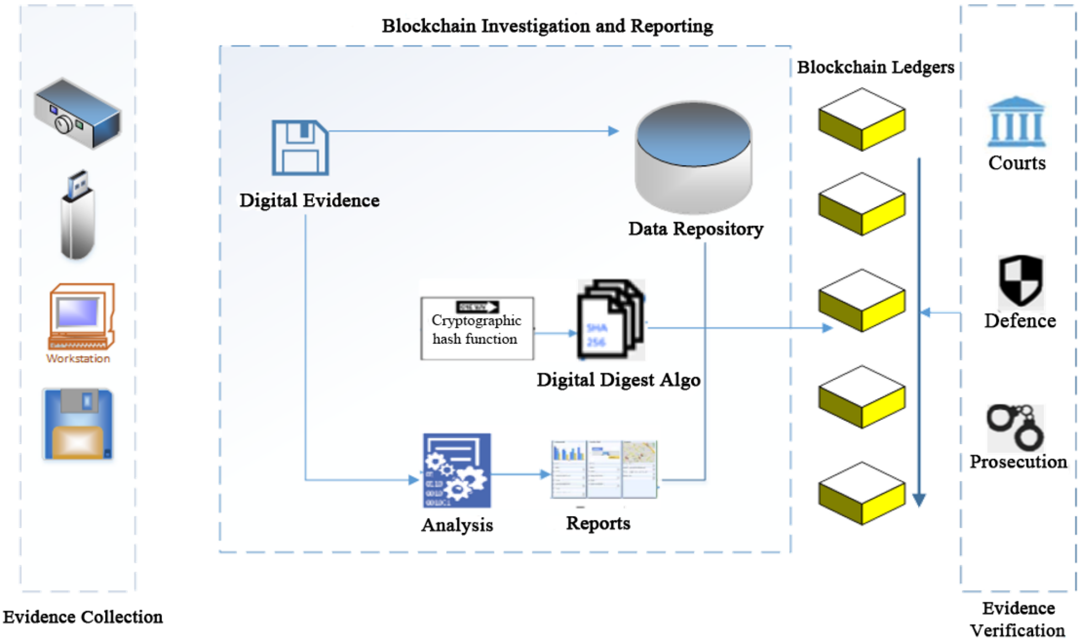

Figure 3. Blockchain forensics investigation

Privacy-centric cryptocurrencies, notably Monero and Zcash, have become subjects of intense scrutiny within the precincts of cryptocurrency forensics. Intrinsically designed to veil transactional specifics and impede fund flow tracking, these currencies have spurred researchers to innovate novel investigatory techniques. Methods ranging from the analysis of transaction histories of interconnected wallets to the deployment of probabilistic techniques for transaction detail inference have been proposed [17, 18].

In tandem with these developments, a growing body of research has been dedicated to harnessing digital footprints for the identification of entities enmeshed in cryptocurrency-centric crimes. Digital imprints have proven invaluable in delineating fund movements between wallets, spotlighting patterns indicative of malfeasance [19, 20]. Such footprints have also facilitated the tracking of individuals resorting to cryptocurrencies for unlawful pursuits, notably dark web marketplace transactions and ransomware offensives.

Interestingly, the domain of cryptocurrency forensics demonstrates considerable overlap with broader financial investigations [21]. Multiple studies have ventured into the applicability of traditional financial investigatory methods in cryptocurrency contexts, encompassing the scrutiny of bank transfers and the detection of facade companies [22]. These investigations have been instrumental in revealing the financial drivers and incentives underpinning cryptocurrency-fueled crimes [20, 23].

An emergent trend in cryptocurrency forensics has been the leveraging of machine learning algorithms for blockchain data evaluation. These algorithms have exhibited proficiency in unveiling patterns of suspicious activity and forecasting impending deceptive transactions [12, 24]. Their prowess extends to handling vast data sets, uncovering correlations potentially elusive to human investigators. Machine learning's potential has been particularly evinced in its adeptness at unmasking cryptocurrency frauds and pyramid schemes, which are incrementally plaguing the cryptocurrency sphere [25].

Supplementing blockchain analysis, efforts have been made to incorporate social network analysis in cryptocurrency forensics. This approach has manifested efficacy, especially when interrogating dark web marketplaces and ransomware onslaughts. In scenarios where criminals deploy intricate networks for fund laundering and identity concealment, social network analysis stands out as a tool enabling investigators to weave connections and pinpoint primary actors in such illicit operations [26, 27].

Furthermore, the domain of cryptocurrency forensics reveals intricate interconnections with the expansive field of cybersecurity. Tools and methodologies, originally conceived by cybersecurity researchers for the deterrence of cyber threats and the fortification of cryptocurrency networks, have found applicability in digital forensic examinations. These instruments have aided in blockchain data analysis and the identification of susceptibilities within the cryptocurrency infrastructure [28–30].

With the escalating trend of cryptocurrency utilization, particularly evident in ransomware incursions and darknet market transactions, the impending era is anticipated to witness intensified synergy between cybersecurity and digital forensics. This collaboration is deemed pivotal in countering the burgeoning menace of cryptocurrency-associated malefactions.

3 Methodological Approach

To decipher the inherent challenges and issues associated with cryptocurrency investigations, over forty articles were reviewed. Comparisons among these articles were conducted to corroborate the identified challenges and issues, ensuring consistency and accuracy. For this research, challenges were perceived as surmountable obstacles that, despite their presence, do not necessarily halt progress. Conversely, issues were interpreted as impediments that hinder the attainment of set objectives.

A comprehensive literature review was undertaken, encompassing reputable academic databases such as IEEE Xplore, ACM Digital Library, and Google Scholar. Keywords, including "cryptocurrency forensics", "digital evidence analysis", and "blockchain investigation", were employed to guarantee an exhaustive selection of relevant publications. Publications were selected based on their alignment with the objectives of this study and their capacity to elucidate the intricacies of cryptocurrency investigation challenges and potential remedies. Emphasis was placed on peer-reviewed journals, conference proceedings, and esteemed publications to ensure the reliability and quality of the sources consulted.

Within the chosen articles, in-depth analysis was performed, extracting pivotal insights, methodologies, and conclusions pertinent to digital evidence investigation within the realm of cryptocurrency. Key data points, techniques, and tools from the investigations were meticulously documented for subsequent comparative analysis. The collated data underwent a rigorous analysis, aiming to uncover recurring themes, challenges, and solutions evident within the body of literature. Approaches employed across various studies were contrasted using qualitative analytical methods, accentuating their merits, limitations, and applicability to real-world scenarios.

4 Results and Implications

From the comprehensive review of literature, several pivotal challenges and issues pertaining to the investigation of cryptocurrencies as digital evidence were identified and are delineated as follows.

4.1 Inherent Challenges in Cryptocurrency Investigations

Owing to the decentralized attributes of cryptocurrency networks coupled with transactional anonymity, it is discerned that investigations into cryptocurrency-associated illicit activities demand distinct knowledge and techniques. These techniques are distinct from those traditionally utilized in financial inquiries. The ability to trace and discern transaction patterns, while navigating the intricate technical underpinnings of cryptocurrencies, has been highlighted [31, 32].

4.2 Emphasis on Blockchain Analytical Tools

For surmounting the intricacies of cryptocurrency probes, reliance on specialized blockchain analytical tools has been observed [33]. Such tools have been reported to facilitate the tracing of transactions and the identification of involved parties, streamlining the case-building process against entities embroiled in malfeasance [34, 35].

4.3 Imperative for Stakeholder Collaboration

It has been noted that the multifaceted nature of cryptocurrency investigations necessitates collaboration. Specifically, law enforcement entities, financial establishments, and cybersecurity experts must converge [36]. The expertise in diverse realms such as digital forensics, fiscal analysis, and legal adherence has been emphasized, with collaborations regarded as paramount in countering cryptocurrency challenges [37].

4.4 The Predicament of Money Laundering

The anonymity inherent in transactions and the paucity of regulatory measures in the cryptocurrency arena render money laundering a profound concern in probes [38, 39]. Nevertheless, enhancements in blockchain analytical tools are progressively equipping investigators to pinpoint suspicious transactions and isolate the involved parties [40].

4.5 Regulatory Flux

Global governmental efforts to formulate cryptocurrency regulations aiming to deter malefactions and shield consumers have been recognized [41, 42]. It is anticipated, based on trends, that as the gravitas of cryptocurrencies amplifies, regulatory architectures will adapt in tandem [43].

4.6 Continuous Learning: A Prerequisite

The brisk technological trajectory in the cryptocurrency domain signifies an imperative for perpetual learning among investigators [44, 45]. The significance of continual training to remain abreast of novel tools and methodologies is underscored.

4.7 Economic and Temporal Implications of Probes

It is indicated that due to the labyrinthine infrastructure of cryptocurrencies and the exigencies of specialized tools, the fiscal and temporal commitments in cryptocurrency inquiries tend to overshadow those of conventional financial investigations [31]. However, the enormity of potential financial repercussions from cryptocurrency-related transgressions underscores the imperativeness of these probes [46].

4.8 Evolutionary Nature of Cryptocurrency Forensics

As cryptocurrencies cement their mainstream stature, the field of cryptocurrency forensics is ascertained to be in flux. The advent of innovative tools and methodologies tailored to the singularities of cryptocurrency probes is documented. Moreover, endeavors by governmental and enforcement agencies to establish agile regulatory frameworks commensurate with the dynamic cryptocurrency milieu are noted [31].

Further research might delve deeper into the evolution of tools and techniques, probing their efficacy and potential pitfalls in the swiftly mutating landscape of cryptocurrency investigations.

5 Proposed Solutions in Response to Identified Challenges

Arising from the challenges elucidated in Section 4, a suite of proposed resolutions has been outlined, as shown in Table 1.

Table 1. Issues, challenges, and recommended solutions

Sr#	Issue and Challenges	Recommended Solutions
1	Unique challenges in cryptocurrency investigations	Prioritize investments in specialized training, resources, and blockchain analysis tools, notably Chainalysis, CipherTrace, and Elliptic.
2	Necessity of specialized blockchain analysis tools	Encourage law enforcement and financial institutions to fund specialized training and maintain updated blockchain analytical instruments.
3	Essential collaboration among stakeholders	Institutionalize routine meetings, intel exchanges, and collaborative training sessions between law enforcement, financial entities, and cybersecurity experts.
4	Money laundering in cryptocurrency investigations	Advocate for robust regulatory edicts for cryptocurrency platforms, emphasizing strict adherence to KYC and AML norms. Employ sophisticated analytics for monitoring.
5	The dynamic nature of regulatory frameworks	Governments are advised to be agile, periodically updating regulations in light of emerging trends like DeFi and NFTs.
6	Continuous learning imperative in cryptocurrency probes	Stakeholders in cryptocurrency forensics are urged to engage in ongoing education, emphasizing participation in symposia, seminars, and training modules.
7	Resource intensity of cryptocurrency investigations	Bolster inter-agency collaboration and intel sharing. Regulatory bodies should strategically allocate resources towards specialized units and analytical tools.
8	Rapid evolution in cryptocurrency forensics	Emphasize the need for continuous academic and practical engagement for experts, including scholarly readings, research endeavors, and industry collaborations.

5.1 Addressing the Unique Challenges in Cryptocurrency Investigations

For the effective surmounting of cryptocurrency investigation hurdles, investment in specialized training and tools is advocated. A profound comprehension of cryptocurrency networks, blockchain technologies, and adeptness in digital forensics and financial probes has been underscored. Moreover, the utilization of specific blockchain analysis utilities, notably Chainalysis, CipherTrace, and Elliptic, is deemed indispensable for discerning anomalous transactions and behavioral patterns.

5.2 The Imperativeness of Blockchain Analytical Tools

Emphasizing the earlier point, it is stressed that both law enforcement and financial institutions should earmark funds for acquiring and updating specialized blockchain analytic instruments. By doing so, staying abreast of novel tactics employed by malefactors for obfuscating their illicit endeavors becomes feasible.

5.3 The Pivotal Role of Inter-Agency Collaboration

The indispensability of a collaborative framework involving law enforcement, financial entities, and cybersecurity experts has been accentuated. It is proposed that routine convenings, intel exchange, and symbiotic training initiatives be institutionalized, bolstering collective efficacy against cryptocurrency malfeasance.

5.4 Counteracting Money Laundering in Cryptocurrency Probes

To staunch money laundering within the cryptocurrency ambit, robust regulatory architectures are mooted. Such frameworks should mandate cryptocurrency trading platforms to adhere stringently to Know Your Customer (KYC) and Anti-Money Laundering (AML) stipulations. Concurrently, the acquisition of cutting-edge analytics tools by enforcement agencies is viewed as imperative for flagging and tracking dubious transactions.

5.5 The Fluidity of Regulatory Constructs

In consonance with the capricious nature of the cryptocurrency milieu, regulatory bodies are encouraged to be nimble. Periodic overhauls of extant regulatory edicts, particularly in light of emergent phenomena like decentralized finance (DeFi) and non-fungible tokens (NFTs), are deemed prudent.

5.6 The Continual Learning Curve in Cryptocurrency Investigations

In grappling with the mercurial realm of cryptocurrency forensics, the onus is on investigators and associated stakeholders to perpetually upskill. Engagements such as symposia, seminars, and training interventions are viewed as pivotal in equipping investigators with contemporary investigative modalities.

5.7 Economic and Durational Factors in Cryptocurrency Probes

Efforts to attenuate both fiscal and temporal overheads associated with cryptocurrency investigations are proposed through enhanced inter-agency collaboration and intel dissemination. Simultaneously, the strategic allocation of resources by governance and regulatory agencies, specifically towards specialized investigation cohorts and advanced analytic tools, is highlighted.

5.8 Staying Au Courant in Cryptocurrency Forensics

To remain aligned with the frenetic pace of evolution in cryptocurrency forensics, academicians and industry practitioners are enjoined to maintain a rigorous regimen of self-updation. Such efforts might encompass scholarly reading, research endeavors, and forging synergies with diverse stakeholders within the cryptocurrency ecosystem.

Future exploration might probe deeper into the efficacy of these solutions, providing a feedback loop for refinement and recalibration in alignment with the fluid dynamics of cryptocurrency investigations.

6 Conclusion

Cryptocurrencies, due to their decentralized and anonymous characteristics, have been identified as advantageous tools for illicit activities such as money laundering and fraud. Given their global accessibility, they present unique challenges to both law enforcement agencies and financial institutions. Nevertheless, it has been observed in the literature review that the nascent domain of cryptocurrency forensics displays significant potential to combat these nefarious uses.

Technological advancements and specialized investigative tools, underscored by the importance of continuous education and stakeholder collaboration, are deemed critical for the effective investigation and subsequent prosecution of cryptocurrency-associated malefactions. It is further highlighted that the establishment and rigorous implementation of sturdy regulatory paradigms by governmental and associated bodies are paramount. Such frameworks should mandate cryptocurrency exchanges' strict adherence to KYC and AML regulations, thereby curtailing avenues for monetary malfeasance.

Future prospects in the realm of digital forensics and cryptocurrency inquiries appear promising. Yet, it is suggested that these prospects will hinge on the sustained commitment to research and development in this field. The necessity for enhanced inter-agency communication and data sharing has been consistently emphasized to preemptively address the mutable threats inherent in cryptocurrency-linked illicit activities.

Harnessing the potential advantages of cryptocurrencies, while concurrently mitigating their criminal exploitation, is proposed to cultivate a more secure ecosystem for individuals, enterprises, and the broader economic framework.

Such endeavors, as delineated in this study, may pave the way for a future where the balance between digital currency utility and safety is optimally achieved.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Confilict of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. A. Raza, A. Anwar, and A. H. Khan, “Current issues and challenges with scientific validation of digital evidence,” *Rev. Comput. Eng. Stud.*, vol. 9, no. 3, pp. 111–115, 2022. https://doi.org/10.18280/rces.090304

[2] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, “A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions,” *IEEE Access*, vol. 10, pp. 11 065–11 089, 2022. https://doi.org/10.1109/ACCESS.2022.3142508

[3] S. Kumar, S. Pathak, and J. Singh, “An enhanced digital forensic investigation framework for XSS attack,” *J. Discret. Math. Sci. Cryptogr.*, vol. 25, no. 4, pp. 1009–1018, 2022. https://doi.org/10.1515/comp-2022-0266

[4] R. N. Malvankar and A. Jain, “EnNetForens: An efficient proactive approach for network forensic,” in *2021 International Conference on Communication, Control and Information Sciences (ICCISc)*, Idukki, India, 2021, pp. 1–4. https://doi.org/10.1109/ICCISc52257.2021.9484865

[5] D. Srivasthav, L. Maddali, and R. Vigneswaran, “Study of blockchain forensics and analytics tools,” in *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Paris, France, 2021, pp. 39–40. https://doi.org/10.1109/BRAINS52497.2021.9569824

[6] Y. Wu, A. Luo, and D. Xu, “Forensic analysis of bitcoin transactions,” in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Shenzhen, China, 2019, pp. 167–169. https://doi.org/10.1109/ISI.2019.8823498

[7] Y. Wu, F. Tao, L. Liu, J. Gu, J. Panneerselvam, R. Zhu, and M. N. Shahzad, “A bitcoin transaction network analytic method for future blockchain forensic investigation,” *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1230–1241, 2020. https://doi.org/10.1109/TNSE.2020.2970113

[8] M. Mas’ud, A. Hassan, W. Shah, S. Abdul-Latip, R. Ahmad, A. Ariffin, and Z. Yunos, “A review of digital forensics framework for blockchain in cryptocurrency technology,” in *2021 3rd International Cyber Resilience Conference (CRC)*, Langkawi Island, Malaysia, 2021, pp. 1–6. https://doi.org/10.1109/CRC50527.2021.9392563

[9] M. Zhang, X. Zhang, Y. Zhang, and Z. Lin, “TXSPECTOR: Uncovering attacks in ethereum from transactions,” in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 2775–2792.

[10] S. Kumari, A. Tyagi, and G. Rekha, “Applications of blockchain technologies in digital forensics and threat hunting,” *Recent Trends in Blockchain for Information Systems Security and Privacy*, pp. 159–173, 2021.

[11] J. Nicholls, A. Kuppa, and N. Le-Khac, “Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape,” *IEEE Access*, vol. 9, pp. 163 965–163 986, 2021. https://doi.org/10.1109/ACCESS.2021.3134076

[12] S. Raza, S. Shamim, A. Khan, and A. Anwar, “Intrusion detection using decision tree classifier with feature reduction technique,” *Mehran Univ. Res. J. Eng. Technol.*, vol. 42, no. 2, pp. 30–37, 2023. https://doi.org/10.22581/muet1982.2302.04

[13] A. Heidari and B. Bahrak, “A graph-based deep learning approach for illegal transaction detection in bitcoin,” *Res. Sq.*, 2022. https://doi.org/10.21203/rs.3.rs-2194869/v1

[14] S. Li, T. Qin, and G. Min, “Blockchain-based digital forensics investigation framework in the Internet of Things and social systems,” *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 6, pp. 1433–1441, 2019. https://doi.org/10.1109/TCSS.2019.2927431

[15] E. Chang, P. Darcy, K.-K. R. Choo, and N.-A. Le-Khac, “Forensic artefact discovery and attribution from android cryptocurrency wallet applications,” *arXiv preprint arXiv:2205.14611*, 2022.

[16] S. Hu, S. Zhang, and K. Fu, “Tfchain: Blockchain-based trusted forensics scheme for mobile phone data whole process,” in *2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC)*, Chongqing, China, 2022, pp. 155–165. https://doi.org/10.1109/ITOEC53115.2022.9734408

[17] M. Mirza, A. Ozer, and U. Karabiyik, “Mobile cyber forensic investigations of Web3 wallets on Android and iOS,” *Appl. Sci.*, vol. 12, no. 21, p. 11180, 2022. https://doi.org/10.3390/app122111180

[18] G. Liang, J. Xin, Q. Wang, X. Ni, and X. Guo, “Research on IoT forensics system based on blockchain technology,” *Secur. Commun. Networks*, vol. 2022, pp. 1–14, 2022. https://doi.org/10.1155/2022/4490757

[19] H. Dooney, "The future of art fraud: An artist's memoir," *Griffith Rev.*, no. 79, pp. 111–117, 2023.

[20] M. Qi, Z. Xu, T. Jiao, S. Wen, Y. Xiang, and G. Nan, "A comparative study on the security of cryptocurrency wallets in android system," in *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Wuhan, China, 2022, pp. 399–406. https://doi.org/10.1109/TrustCom56396.2022.00062

[21] J. Prakash, "Cryptocurrency a digital wallet: PRO'S and CON'S," *Int. J. Multidiscip. Educ. Res.*, vol. 11, no. 9, pp. 65–68, 2022.

[22] L. W. Cong, C. R. Harvey, D. Rabetti, and Z. Y. Wu, "An anatomy of crypto-enabled cybercrimes," NBER, Tech. Rep., 2023. https://doi.org/10.2139/ssrn.4188661

[23] S. Salisu and V. Filipov, "Blockchain forensics: A modern approach to investigating cybercrime in the age of decentralisation," in *Proceedings of the 18th International Conference on Cyber Warfare and Security*, Maryland, USA, 2023, pp. 338–347. https://doi.org/10.34190/iccws.18.1.947

[24] N. Pocher, M. Zichichi, F. Merizzi, M. Z. Shafiq, and S. Ferretti, "Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics," arXiv preprint, Tech. Rep., 2022. https://doi.org/10.1007/s12525-023-00654-3

[25] S. Bhardwaj and M. Dave, "Crypto-preserving investigation framework for deep learning based malware attack detection for network forensics," *Wirel. Pers. Commun.*, vol. 122, no. 3, pp. 2701–2722, 2022. https://doi.org/10.1007/s11277-021-09026-6

[26] Z. Ao, G. Horvath, and L. Zhang, "Are decentralized finance really decentralized? A social network analysis of the aave protocol on the ethereum blockchain," arXiv preprint, Tech. Rep., 2022. https://doi.org/10.48550/arXiv.2206.08401

[27] P. K. Shrivastava, "Electronic evidence in crime investigation-darknet & policing," *Indian Police J.*, vol. 68, no. 3, pp. 43–51, 2021.

[28] N. Jain, K. Kaneko, and S. Sharma, "Sklee: A dynamic symbolic analysis tool for ethereum smart contracts (tool paper)," in *Software Engineering and Formal Methods: 20th International Conference, SEFM 2022*, Berlin, Germany, 2022, pp. 244–250. https://doi.org/10.1007/978-3-031-17108-6_15

[29] H. Zhou, A. M. Fard, and A. Makanju, "The state of ethereum smart contracts security: Vulnerabilities, countermeasures, and tool support," *J. Cybersecurity Priv.*, vol. 2, no. 2, pp. 358–378, 2022. https://doi.org/10.3390/jcp2020019

[30] P. D. L. Ivan and C. S. Bădele, "Criptocurencies–The modality of payment of the future. Risks and vulnerabilities," *Rev. Econ. Contemp.*, vol. 6, no. 4, pp. 130–141, 2021.

[31] S. S. Muthye, *Challenges in Digital Forensics and Future Aspects*. Chapman and Hall/CRC, 2023, pp. 75–84.

[32] S. K. Taylor, A. Ariffin, K. A. Z. Ariffin, and S. N. H. S. Abdullah, "Cryptocurrencies investigation: A methodology for the preservation of cryptowallets," in *2021 3rd International Cyber Resilience Conference (CRC)*, Langkawi Island, Malaysia, 2021, pp. 1–5. https://doi.org/10.1109/CRC50527.2021.9392446

[33] Y. Zhou, Y. S. Soh, H. S. Loh, and K. F. Yuen, "The key challenges and critical success factors of blockchain implementation: Policy implications for singapore's maritime industry," *Mar. Policy*, vol. 122, p. 104265, 2020. https://doi.org/10.1016/j.marpol.2020.104265

[34] M. Fröwis, T. Gottschalk, B. Haslhofer, C. Rückert, and P. Pesch, "Safeguarding the evidential value of forensic cryptocurrency investigations," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 200902, 2020. https://doi.org/10.1016/j.fsidi.2019.200902

[35] Y. Sun, H. Xiong, S. M. Yiu, and K. Y. Lam, "BitAnalysis: A visualization system for bitcoin wallet investigation," *IEEE Trans. Big Data*, vol. 9, no. 2, pp. 621–636, 2022. https://doi.org/10.1109/TBDATA.2022.3188660

[36] R. Wu, K. Ishfaq, S. Hussain, F. Asmi, A. N. Siddiquei, and M. A. Anwar, "Investigating e-retailers' intentions to adopt cryptocurrency considering the mediation of technostress and technology involvement," *Sustainability*, vol. 14, no. 2, p. 641, 2022. https://doi.org/10.3390/su14020641

[37] R. Schmid, R. Ziolkowski, and G. Schwabe, "Together or not? Exploring stakeholders in public and permissionless blockchains," in *55th Hawaii International Conference on System Sciences*, Maui, Hawaii, USA, 2022, pp. 6093–6102. https://scholarspace.manoa.hawaii.edu/handle/10125/80079

[38] A. Maurushat and D. Halpin, "Investigation of cryptocurrency enabled and dependent crimes," in *Financial Technology and the Law: Combating Financial Crime*. Springer, 2022, pp. 235–267. https://doi.org/10.1007/978-3-030-88036-1_10

[39] R. M. Zhamiyeva, G. B. Sultanbekova, M. T. Abzalbekova, B. A. Zhakupov, and M. G. Kozhanov, "The role of financial investigations in combating money laundering," *Int. J. Electron. Secur. Digit. Forensics*, vol. 14, no. 2, pp. 188–198, 2022. https://doi.org/10.1504/IJESDF.2022.121183

[40] S. Seo, B. Seok, and C. Lee, "Digital forensic investigation framework for the metaverse," *J. Supercomput.*, vol. 79, pp. 9467–9485, 2023. https://doi.org/10.1007/s11227-023-05045-1

[41] M. Hosen, H. M. T. Thaker, V. Subramaniam, H. C. Eaw, and T. H. Cham, "Artificial Intelligence (AI), blockchain, and cryptocurrency in finance: Current scenario and future direction," in *International Conference on Emerging Technologies and Intelligent Systems*, 2022, pp. 322–332. https://doi.org/10.1007/978-3-031-25274-7_26

[42] G. Gunarso, "Cryptocurrency and its state of research," *Int. Dialogues Educ. J.*, vol. 9, no. 1, pp. 151–175, 2022. https://doi.org/10.53308/ide.v9i1.280

[43] D. J. Cumming, S. Johan, and A. Pant, "Regulation of the crypto-economy: Managing risks, challenges, and regulatory uncertainty," *J. Risk Financ. Manag.*, vol. 12, no. 3, p. 126, 2019. https://doi.org/10.3390/jrfm12030126

[44] C. Horan and H. Saiedian, "Cyber crime investigation: Landscape, challenges, and future research directions," *J. Cybersecurity Priv.*, vol. 1, no. 4, pp. 580–596, 2021. https://doi.org/10.3390/jcp1040029

[45] E. Casey and A. Zehnder, "Inter-Regional digital forensic knowledge management: Needs, challenges, and solutions," *J. Forensic Sci.*, vol. 66, no. 2, pp. 619–629, 2021. https://doi.org/10.1111/1556-4029.14613

[46] M. Li, C. Lal, M. Conti, and D. Hu, "Lechain: A blockchain-based lawful evidence management scheme for digital forensics," *Future Gener. Comput. Syst.*, vol. 115, pp. 406–420, 2021. https://doi.org/10.1016/j.future.2020.09.038