Asia-Pacific Journal of Information Technology and Multimedia 14(2) 2025: 585 – 594
https://doi.org/10.17576/apjitm-2025-1402-15

Forensic Analysis of Cryptocurrencies: A Comprehensive Overview

Analisis Forensik Mata Wang Kripto: Tinjauan Komprehensif

Noor Hazfalinda Hamzah[1], Khairul Osman[1], Qi Wei Kong[1], Atikah Mohd Nasir[1], Nur Mahiza Md Isa[2]*

[1]Forensic Science Programme, Faculty of Health Sciences, Basement 1, Perpustakaan Tun Seri Lanang, 43600 Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia

[2]Jabatan Patologi & Mikrobiologi Veterinar, Fakulti Perubatan Veterinar, Universiti Putra Malaysia, 43400 Universiti Putra Malaysia, Serdang, Selangor, Malaysia

[*]Corresponding author: raviera@yahoo.com

Received 26 March 2025
Accepted 1 October 2025, Available online 15 December 2025

ABSTRACT

The rapid proliferation of cryptocurrencies has revolutionised digital transactions, but their pseudonymous nature poses significant challenges for forensic investigations of illicit activities like money laundering and fraud. While blockchain's transparency enables transaction tracing, advanced obfuscation techniques (e.g., mixers, privacy coins) and the lack of standardised forensic protocols hinder law enforcement efforts. This study systematically reviews current blockchain forensic tools (e.g., Chainalysis, Elliptic) and analysis techniques (heuristic clustering, AI-driven anomaly detection) to evaluate their efficacy across the forensic investigation lifecycle: identification, preservation, analysis, and presentation. We identify critical gaps in addressing privacy-enhanced cryptocurrencies and inconsistent admissibility of digital evidence in court. By synthesising these findings, we propose actionable recommendations for developing a unified forensic framework that integrates technical robustness with legal compliance, ensuring reliable evidence for prosecution. Our analysis underscores the urgent need for international collaboration and regulatory alignment to combat evolving cryptocurrency-related crimes. This paper contributes by synthesising existing methods, identifying gaps, and proposing a unified forensic framework suitable for judicial contexts.

Keywords: Cryptocurrency Forensics, Blockchain Analysis, Digital Currency Investigations, Bitcoin Forensics, Ethereum Tracing

ABSTRAK

Penyebaran pesat mata wang kripto telah merevolusikan transaksi digital, tetapi sifat samar-samar (pseudonymous) menimbulkan cabaran yang ketara untuk siasatan forensik terhadap aktiviti haram seperti pengubahan wang haram dan penipuan. Walaupun ketelusan blok rantai (blockchain) membolehkan pengesanan transaksi, teknik pengaburan canggih (contohnya, "*mixers*", "*privacy coins*") dan kekurangan protokol forensik yang seragam menghalang usaha penguatkuasaan undang-undang. Kajian ini mengulas secara sistematik alat forensik blok rantai semasa (contohnya, Chainalysis, Elliptic) dan teknik analisis (pengelompokan heuristik, pengesanan anomali dipacu AI) untuk menilai keberkesanannya merentasi kitaran hayat siasatan forensik: pengenalpastian, pemeliharaan, analisis, dan pembentangan. Kami mengenal pasti jurang kritikal dalam menangani mata wang kripto yang dipertingkatkan privasi dan kebolehterimaan bukti digital yang tidak konsisten di mahkamah. Dengan mensintesis penemuan ini, kami mencadangkan tindakan yang boleh diambil untuk membangunkan rangka kerja forensik yang menggabungkan keteguhan teknikal dengan pematuhan undang-undang, bagi memastikan bukti yang boleh dipercayai untuk pendakwaan. Analisis kami menggariskan keperluan mendesak untuk kerjasama antarabangsa dan penyelarasan peraturan untuk memerangi jenayah berkaitan mata wang kripto yang semakin berkembang. Artikel ini menyumbang dengan mensintesis kaedah sedia ada, mengenal pasti jurang, dan mencadangkan rangka kerja forensik bersepadu yang sesuai untuk konteks kehakiman.

Kata kunci: Forensik Mata Wang Kripto, Analisis Rantai Blok, Siasatan Mata Wang Digital, Forensik Bitcoin, Pengesanan Ethereum

INTRODUCTION

The rapid rise of cryptocurrencies has transformed financial ecosystems, offering users decentralised and borderless means of exchange. Unlike traditional financial systems, which operate under regulated institutions, cryptocurrencies are based on distributed ledger technology where transactions are pseudonymous, permanent, and immutable (Narayanan et al., 2016). These characteristics, while innovative, present significant challenges for investigators. Criminal groups exploit the anonymity of blockchain networks to conduct illicit activities, including money laundering, ransomware payments, narcotics trade, and human trafficking (Foley et al., 2018). Investigators are thus confronted with the dual task of preserving the innovative use of cryptocurrencies in legitimate commerce while developing forensic techniques robust enough to detect, trace, and prosecute criminal misuse.

A central difficulty lies in balancing technical accuracy with legal admissibility. Blockchain transactions generate extensive digital traces, yet the translation of these technical findings into courtroom-acceptable evidence is not straightforward. In many jurisdictions, digital evidence must meet strict admissibility standards to be considered valid. In the United States, for instance, the *United States v. Harmon* case highlighted the judiciary's demand for rigorous forensic methods to ensure that cryptocurrency tracing could withstand Daubert standards, which require scientific validity and reliability (Court Listener, 2020). However, many Asian jurisdictions, including Malaysia, do not follow Daubert or Frye tests. Instead, admissibility hinges on provisions in the Evidence Act 1950, which requires that forensic evidence be both relevant and

obtained through legally recognised procedures. This creates a pressing need for frameworks that ensure blockchain forensic methods are not only technologically sound but also legally defensible in diverse judicial contexts.

Without harmonising technical precision with legal requirements, blockchain forensic evidence risks dismissal, even in cases involving serious financial crime. This risk is compounded in regions where regulatory infrastructures around cryptocurrency are still developing. In Malaysia, for example, cryptocurrency is regulated under the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019, which brings digital assets under the purview of the Securities Commission Malaysia. While this regulation governs the use and trading of cryptocurrencies, it does not explicitly address forensic standards or evidentiary admissibility in criminal cases, leaving a gap between financial oversight and forensic application (Securities Commission Malaysia, 2019).

Case studies across the Asia-Pacific illustrate these challenges. In 2019, Singapore's Commercial Affairs Department successfully prosecuted a S$24 million fraud case by tracing Bitcoin transactions to local exchanges using Chainalysis tools—a landmark demonstration of blockchain forensics' validity under the Payment Services Act (Monetary Authority of Singapore, 2019). Conversely, in jurisdictions with weaker institutional frameworks, cryptocurrency investigations often fail to progress due to the absence of standardised forensic procedures. These disparities underscore the need for a harmonized forensic approach tailored to regional legal systems.

This paper responds to these challenges by offering a comprehensive review of blockchain forensic techniques and their alignment with legal admissibility. By critically examining tools, methodologies, and case applications, it highlights the gap between forensic innovation and courtroom standards in the Asia-Pacific context. The objective is not only to map existing forensic strategies but also to emphasize the importance of integrating technical robustness with judicial acceptance, ensuring that blockchain evidence serves its intended role in both investigation and prosecution.

The manuscript is structured as follows: Section 2 discusses the blockchain forensic tools and their relevance to forensic stages. Section 3 analyses various analytical techniques used in cryptocurrency investigations. Section 4 highlights regulatory and evidentiary challenges. Section 5 highlights the need for standardised blockchain forensic frameworks and strengthened regulatory. The final section concludes with recommendations for future research and standardisation efforts.

BLOCKCHAIN FORENSICS – TOOLS AND TECHNIQUES

Modern blockchain forensic investigations employ a structured approach that aligns with traditional digital forensic phases while addressing the unique challenges of decentralized systems. The process begins with identification, where specialised tools like Chainalysis Reactor and Elliptic Navigator scan public blockchain data to detect suspicious patterns. These platforms function as the cryptocurrency equivalent of open-source intelligence (OSINT) gathering, applying heuristic techniques such as the multiple-input rule to cluster related addresses. For

instance, during the DarkSide ransomware investigation, these methods successfully linked 87% of the illicit transactions to known criminal wallets (Raza Shirazi et al., 2023). However, the effectiveness of these techniques diminishes when facing sophisticated privacy tools, highlighting the ongoing arms race between forensic investigators and blockchain obfuscation technologies.

The preservation phase capitalises on blockchain's inherent immutability but requires meticulous protocols to maintain evidentiary integrity. Tools like CipherTrace's forensic suite create auditable custody chains that document every interaction with the digital evidence, satisfying legal standards for chain of custody (Wagman, 2022). This process becomes particularly challenging with privacy-focused cryptocurrencies; Monero's ring signatures, for example, have been shown to reduce traceability by over 70% compared to transparent blockchains like Bitcoin (Biryukov & Tikhomirov, 2019). Recent Europol reports indicate that only about 12% of Monero transactions can be fully reconstructed using current forensic methods, underscoring the need for continued innovation in this area (EUROPOL, 2022).

Analysis represents the most technically complex stage, where artificial intelligence and network science converge to unravel transaction patterns. Machine learning models developed by companies like Elliptic analyse vast transaction networks to assign risk scores, while Graph Neural Networks map the intricate web of money flows across wallets and exchanges (Hamilton & Leuprecht, 2024). These advanced techniques, however, face scepticism in legal settings due to their complexity. The Mt. Gox hack investigation demonstrated this tension clearly - while forensic analysts successfully traced hundreds of thousands of stolen bitcoins, courts frequently challenged the statistical methods used to establish address linkages (Reddy & Minnaar, 2018). This judicial hesitancy reflects broader concerns about the admissibility of novel scientific evidence under standards like Frye and Daubert.

The final presentation stage bridges the gap between technical analysis and legal requirements. The Five T Model (Transparency, Traceability, Tracking, Transferability, and Trust) provides a framework for transforming complex blockchain data into compelling courtroom evidence (Almahadeen et al., 2024). This approach emphasizes clear documentation of methodologies, visual representation of money flows, and peer validation of forensic tools. Yet significant challenges remain, particularly with technologies like CoinJoin mixers that can reduce Bitcoin traceability to as little as 22% (Liu et al., 2021) and zero-knowledge proof systems that offer complete transaction privacy. Emerging solutions such as cross-chain analysis AI and regulatory sandbox environments for testing new forensic methods promise to address these limitations while ensuring compliance with evolving international standards like the Financial Action Task Force (FATF) Travel Rule (Salisu & Filipov, 2023).

ANALYSIS TECHNIQUES IN BLOCKCHAIN FORENSICS: FROM TRANSACTION TRACING TO BEHAVIORAL PROFILING

Forensic analysis of cryptocurrency is a multidisciplinary approach that focuses on tracking and interpreting the flow of digital assets within blockchain networks. Although blockchain is designed to provide pseudonymity, it does not guarantee complete anonymity. Each user is represented by unique wallet addresses and cryptographic hash strings that, while concealing

direct identity can still be analysed to uncover linkages between users, transactions, and networks (Salisu & Filipov, 2023). This duality, pseudonymity combined with traceable transaction data makes blockchain forensics both complex and promising. The foundation of this forensic work lies in transaction tracing and address linkage, which requires sophisticated tools to investigate the origin of funds, the sequence of transfers, and the ultimate destinations. Three dominant analytical perspectives guide current research and practices are traceability and linkability of transactions, collective transaction patterns within blockchain networks, and behavioral profiling of individual users.

TRACEABILITY AND LINKABILITY IN BLOCKCHAIN TRANSACTIONS

Tracing cryptocurrency transactions involves uncovering how funds move through the blockchain and identifying relationships between seemingly independent wallet addresses. Techniques such as statistical analysis and graphical visualisation are employed to extract abnormal transaction flows, illicit activity patterns, and suspicious address linkages (Nicholls, Kuppa, & Le-Khac, 2023). Graph Neural Networks (GNNs) have emerged as a powerful tool, enabling forensic investigators to generate graph embeddings that represent nodes (addresses) and edges (transactions) for downstream tasks such as anomaly detection and classification. These methods have been instrumental in high-profile investigations involving ransomware, human trafficking, sextortion, and dark web marketplaces.

To evade detection, criminals often rely on countermeasures such as mixing services, privacy-focused altcoins, and other obfuscation strategies designed to conceal the origin and destination of funds. In response, forensic researchers have introduced taint analysis methods that apply a series of heuristics to trace and link transactions. These heuristics include the multiple-input rule, which assumes that all input addresses in a transaction are controlled by the same user; the coin change rule, which posits that any excess value in a transaction is typically returned to the sender’s address; and the zero-mix rule, which allows investigators to identify real spends in privacy-enhancing cryptocurrencies such as CryptoNote by detecting closed transaction sets (Liu et al., 2021).

Another advanced technique, subset-sum matching, matches input-output pairs in transactions by analysing identical or near-identical transfer values. This method has been particularly effective in countering mixing services, as many users inadvertently reveal transaction linkages by withdrawing and depositing equivalent amounts (Liu et al., 2021). Collectively, these techniques enhance the ability of forensic analysts to pierce through pseudonymity barriers.

COLLECTIVE TRANSACTION PATTERNS IN BLOCKCHAIN NETWORKS

The second analytical approach involves examining network-wide transaction structures. Blockchain inherently forms a decentralised, peer-to-peer network, where nodes represent participants and edges signify transactions. Each block contains a timestamp, cryptographic hash, and a chain link to the previous block, ensuring immutability and traceability (Bonomi et al., 2018). By studying the topology and evolution of this network, investigators can identify clusters of illicit activity and map collective transaction behaviours.

For example, transaction clustering algorithms can identify rings of addresses controlled by a single entity, such as ransomware operators or darknet markets. Similarly, abnormal transaction density between specific nodes may suggest money laundering operations. The structural analysis of nodes and edges also provides insights into systemic risks, such as how illicit activity spreads across interconnected wallets. Network science techniques, therefore, provide a macro-level forensic perspective, complementing address-level analysis and enhancing situational awareness for regulators and law enforcement.

BEHAVIOURAL ANALYSIS OF BLOCKCHAIN USERS

The most nuanced dimension of blockchain forensics involves behavioural analysis, which seeks to classify user identities and detect malicious actors through their digital footprints. One widely adopted technique is address tagging, where investigators associate wallet addresses with known individuals or organisations using open-source data such as online forums, exchange disclosures, or voluntary posts by users (Liu et al., 2021). Once tagged, these addresses enable the construction of behavioural networks linking multiple wallets to a single identity.

User profiling in blockchain forensics extends beyond simple address tagging and incorporates the analysis of a range of transactional features. These features include volume features, which focus on the amount and size of transactions; temporal features, which examine transaction frequency, periodicity, and timing; and network position features, which evaluate an address's centrality or influence within the transaction graph. In addition, for blockchains that support smart contracts, such as Ethereum, user profiling can also leverage contract interactions by analyzing the types of decentralized applications or contracts associated with a given address. Together, these features provide investigators with a deeper understanding of user behaviours and enable the detection of suspicious or illicit activities with greater accuracy.

Signature behaviours, such as peeling chains (splitting large sums into smaller, repeated transfers) or consistent reliance on mixers, provide identifiable red flags. Advanced approaches integrate machine learning and AI, especially GNNs and anomaly detection models, to classify transaction sequences and uncover deviations from expected patterns (Akcora et al., 2019). This form of forensic profiling not only enables the identification of high-risk addresses but also contributes to predictive models for anticipating future illicit activity.

Collectively, these three layers of forensic analysis; transaction linkability, collective transaction patterns, and behavioural profiling form a comprehensive toolkit for investigators. Traceability establishes the where of cryptocurrency flows, collective patterns reveal the how at a systemic level, and behavioural analysis provides the who behind suspicious activities. This integration of network science, AI-driven analytics, and forensic heuristics advances both the scientific study and the practical application of blockchain forensics.

COMPARATIVE ANALYSIS OF FORENSIC METHODS: HEURISTIC VS. AI-BASED APPROACHES

Blockchain forensic methodologies are broadly classified into heuristic-based techniques and AI-driven approaches, each with distinct advantages and limitations in tracking illicit transactions. Heuristic-based methods rely on predefined rules to cluster addresses and identify suspicious

activities. Common heuristics include the multi-input rule, which assumes that multiple input addresses in a transaction are controlled by the same entity (Meiklejohn et al., 2016), and the change address rule, which identifies outputs likely belonging to the sender. Other heuristic techniques, such as the peeling chain heuristic, detect money laundering strategies where large sums are systematically broken down over multiple transactions (Zhang et al., 2020). While these methods are widely used in commercial forensic tools like Chainalysis and Elliptic due to their computational efficiency and ease of implementation, they struggle against modern obfuscation techniques like coin mixing, CoinJoin, and privacy wallets (Biryukov & Tikhomirov, 2019). Moreover, heuristic models are static and rule-based, meaning they cannot detect emerging money laundering techniques that do not conform to known transaction patterns.

To overcome these limitations, AI-driven forensic models have emerged, leveraging machine learning and deep learning to identify hidden patterns in blockchain transaction data. One of the most effective AI methods is GNNs, which model the blockchain as a transaction graph, allowing forensic analysts to detect fraudulent transactions based on structural anomalies (Akcora et al., 2019). AI-based anomaly detection algorithms can dynamically flag illicit activities by recognizing transaction behaviours that deviate from typical user patterns. Clustering algorithms such as K-Means and DBSCAN are also used to group blockchain addresses with similar transaction histories, improving accuracy in identifying illicit networks. Additionally, Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) models have been applied to predict future suspicious transactions based on past behaviours (Weber et al., 2019). Compared to heuristic methods, AI-based models offer significantly higher detection accuracy, reaching 92% in some studies, compared to 75–85% for heuristics (Biryukov & Tikhomirov, 2019; Weber et al., 2019). AI models are particularly effective at detecting novel laundering techniques and analysing large-scale blockchain data. However, they require large labelled datasets for training, are computationally intensive, and lack interpretability, which makes them challenging to present as legal evidence in forensic investigations.

Despite their differences, both forensic approaches play a critical role in blockchain investigations**.** Heuristic methods remain the preferred choice in real-world forensic applications due to their simplicity, speed, and legal admissibility. They are widely implemented in financial regulatory compliance and law enforcement investigations where clear, rule-based evidence is necessary (Foley et al., 2018). In contrast, AI-driven methods are increasingly used in proactive financial crime detection, particularly by cryptocurrency exchanges and cybersecurity firms to flag high-risk accounts. Future forensic advancements are likely to involve a hybrid approach, combining the efficiency and legal robustness of heuristics with the adaptability and accuracy of AI models. As blockchain technology evolves, forensic analysts will need adaptive methodologies capable of detecting sophisticated money laundering and fraud strategies, particularly in DeFi and privacy-focused cryptocurrencies.

In summary, Table 1 depicts the comparative analysis of forensic methods (heuristic vs. AI-based) (Akcora et al., 2019).

TABLE 1. The comparative analysis of forensic methods (heuristic vs. AI-based)

Forensic Technique	Methodology	Strengths	Limitations	Detection Accuracy
Heuristic-Based Clustering	Multi-input rule, address reuse	Simple, computationally efficient	Fails against coin mixing techniques	75-85%
AI-Driven Anomaly Detection	Deep learning on transaction patterns	High precision, adaptable	Requires large training datasets	90-95%
Network Graph Analysis	Detects transaction relationships	Effective for large-scale fraud	Computationally expensive	85-90%

TOWARD A STANDARDISED FORENSIC FRAMEWORK AND REGULATORY ALIGNMENT

The growing sophistication of cryptocurrency-related crimes demands equally advanced forensic solutions, but current approaches remain fragmented. While tools like Chainalysis and Elliptic offer powerful tracing capabilities, their proprietary methods often produce inconsistent results that may not meet legal evidentiary standards (Atlam et al., 2024) as in Table 2. This inconsistency is especially problematic for privacy coins like Monero, where traditional tracing methods fail entirely (Biryukov & Tikhomirov, 2019). To bridge this gap, we propose a unified framework built on four pillars: technical robustness, legal compliance, regulatory collaboration, and adaptive innovation.

Technical Protocols form the foundation. Open-source forensic tools with transparent validation metrics (e.g., ≥90% detection rates for AI models) could reduce discrepancies between platforms. Cross-chain analysis capabilities are equally critical, as criminals increasingly move funds across multiple blockchains to evade detection (Nicholls et al., 2023). For example, Graph Neural Networks (GNNs) have shown promise in tracing such complex flows but require standardisation to ensure courtroom admissibility (Akcora et al., 2019).

Legal Compliance is equally vital. Courts often reject digital evidence due to unclear chain-of-custody documentation or unvalidated forensic methods (Almahadeen et al., 2024). Blockchain-native timestamps and alignment with the Daubert Standard which requires scientific reliability—could address this. The 2014 Mt. Gox hack investigation demonstrated how poor evidence handling led to irreversible losses, while the Silk Road case succeeded due to meticulous tracing (Foley et al., 2018; Reddy & Minnaar, 2018).

Regulatory Collaboration must extend beyond borders. The FATF's Travel Rule, which mandates identity sharing for crypto transactions, is a start but DeFi platforms often bypass these requirements (Wagman, 2022). Harmonising global AML/ Counter-Terrorist Financing regulations and mandating real-time reporting of suspicious transactions could close these loopholes.

Finally, Continuous Adaptation ensures the framework evolves with emerging threats. Zero-knowledge proofs and Layer-2 solutions like Lightning Network already challenge existing tools (Liu et al., 2021). A dedicated forensic Research and Development (R&D) fund, similar to cybersecurity initiatives, could spur innovation in countering these techniques.

TABLE 2. Forensic Tools Compliance with Proposed Framework

Tool	Technical Protocols (Open-source/Cross-chain)	Legal Compliance (Daubert-Admissible)	Regulatory Alignment (FATF Travel Rule)	Adaptive Innovation (Monero/Zcash Support)
Chainalysis	Limited (Proprietary)	Partial (Peer-reviewed)	Yes	No (Limited privacy-coin tracing)
Elliptic	No	Yes	Partial	Emerging AI models
CipherTrace	Partial (Cross-chain)	Yes	Yes	Yes (Basic Monero analysis)

CONCLUSION

In conclusion, this study demonstrates that blockchain forensic techniques, particularly AI-driven anomaly detection, significantly enhance transaction tracking accuracy compared to heuristic clustering. However, the absence of a unified forensic framework remains a challenge, leading to inconsistencies in digital crime investigations. Future research should focus on developing standardised forensic protocols that integrate AI, network graph analysis, and legal enforcement mechanisms. Additionally, the rise of privacy coins and Layer 2 scaling solutions (such as Lightning Network) necessitates adaptive forensic methodologies that can overcome obfuscation techniques. The findings of this study provide valuable insights for forensic experts, regulatory agencies, and cybersecurity professionals, advocating for a more structured approach to blockchain forensic investigations.

REFERENCES

Akcora, C., Li, Y., Gel, Y., & Kantarcioglu, M. 2019. BitcoinHeist: Topological Data Analysis for Ransomware Detection on the Bitcoin Blockchain. *arXiv:1906.07852*, 1-15. doi:10.48550/arXiv.1906.07852.

Almahadeen, L., Pecho, R. D. C., Raj, M. G., Rajesh, N., Mohammed Imneef, Z., & Yelpale, S. K. 2024. Digital Investigation Forensic Model with P2P Timestamp Blockchain for Monitoring and Analysis. *Journal of Electrical Systems*, 20(1), 9. doi:https://doi.org/10.52783/jes.656.

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), 3568.

Biryukov, A., & Tikhomirov, S. 2019, 17-19 June 2019. *Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis.* Paper presented at the 2019 IEEE European Symposium on Security and Privacy (EuroS&P).

Bonomi, S., Casini, M., & Ciccotelli, C. 2018. *B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics*.

Court Listener. 2020. United States v. Harmon. Retrieved from https://www.courtlistener.com/opinion/4843029/united-states-v-harmon/?q=cites%3A109687.

EUROPOL. 2022. Cryptocurrencies: tracing the evolution of criminal finances. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%

20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf.

Foley, S., Karlsen, J. R., & Putnins, T. J. 2018. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *Review of Financial Studies, Forthcoming*. doi:http://dx.doi.org/10.2139/ssrn.3102645.

Hamilton, R., & Leuprecht, C. 2024. The Crime-Crypto Nexus: Nuancing Risk Across Crypto-Crime Transactions. In D. Goldbarsht & L. de Koker (Eds.), *Financial Crime and the Law: Identifying and Mitigating Risks* (pp. 15-42). Cham: Springer Nature Switzerland..

Liu, X. F., Jiang, X. J., Liu, S. H., & Tse, C. K. 2021. Knowledge Discovery in Cryptocurrency Transactions: A Survey. *IEEE Access*, 9, 37229-37254. doi:10.1109/ACCESS.2021.3062652.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. 2016. A fistful of Bitcoins: characterizing payments among men with no names. *Commun. ACM*, 59(4), 86–93. doi:10.1145/2896384.

Monetary Authority of Singapore. 2019. Enforcement of payment services regulations. Retrieved from https://www.dlapiperintelligence.com/export/sites/intelligence-old/investmentrules/blog/articles/2019/Downloads/b2c2-ltd-v-quoine-pte-ltd_a1cd5e6e-288e-44ce-b91d-7b273541b86a_8de9f2e2-478e-46aa-b48f-de469e5390e7.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*: Princeton University Press.

Nicholls, J., Kuppa, A., & Le-Khac, N.-A. 2023. *FraudLens: Graph Structural Learning for Bitcoin Illicit Activity Identification*. Paper presented at the Proceedings of the 39th Annual Computer Security Applications Conference, Austin, TX, USA. https://doi.org/10.1145/3627106.3627200.

Raza Shirazi, S., Shaikh, M., & Tahira, K. 2023. Cryptocurrency Investigations in Digital Forensics: Contemporary Challenges and Methodological Advances. *Information Dynamics and Applications*, 2, 126-134. doi:10.56578/ida020302.

Reddy, E., & Minnaar, A. 2018. Cryptocurrency : a tool and target for cybercrime. *Acta Criminologica : African Journal of Criminology & Victimology,* 31(3), 71-92. doi:doi:10.10520/EJC-14d902942d.

Securities Commission Malaysia. 2019. Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019. Retrieved from https://www.sc.com.my/api/documentms/download.ashx?id=8c8bc467-c750-466e-9a86-98c12fec4a77.

Wagman, S. 2022. Cryptocurrencies and National Security: The Case of Money Laundering and Terrorism Financing. *Harvard National Security Journal*, 14, 87-102.

Weber, M., Domeniconi, G., Chen, J., Weidele, D., Bellei, C., Robinson, T., & Leiserson, C. 2019. *Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics*. Paper presented at the KDD '19 Workshop on Anomaly Detection in Finance, Anchorage, AK, USA. https://www.researchgate.net/publication/335028528_Anti-Money_Laundering_in_Bitcoin_Experimenting_with_Graph_Convolutional_Networks_for_Financial_Forensics.

Zhang, Y., Wang, J., & Luo, J. 2020. Heuristic-Based Address Clustering in Bitcoin. *IEEE Access*, 8, 210582-210591. doi:10.1109/ACCESS.2020.3039570.