Blockchain Forensics - Unmasking Anonymity in Dark Web Transactions

Jelena Gjorgjev[1,*], M.F. Fajar Ramadhan[2] and Sonny Dhamayana[3]

[1]*Brainster Next College, Skopje, North Macedonia*

[2]*University of Gadjah Mada Math and Science Faculty Electronic and Computer Science Department Yogyakarta, Indonesia*

[3]*Alternative Control Labs FZC, Dubai, UAE*

Abstract: This paper analyzes the impact of blockchain forensic techniques on combating cybercrime in the dark web. Although cryptocurrencies were originally celebrated for their decentralized and anonymous characteristics, advancements in blockchain analytics have allowed law enforcement agencies to track unlawful transactions with greater precision. This paper investigates forensic techniques including clustering, heuristic analysis, and address tagging to identify offenders involved in money laundering, drug trafficking, and ransomware transactions. This paper examines real-world case studies, including as the dismantling of Silk Road and Chainalysis's involvement in tracing illicit wallets, to illustrate the dynamic adversarial relationship between cybercriminals and law enforcement agencies. It also addresses the legal and ethical dilemmas associated with blockchain surveillance. The findings indicate that although blockchain forensics has markedly advanced cybercrime investigations, the emergence of privacy-enhancing technologies presents new challenges necessitating policy adjustments.

Keywords: Blockchain forensics, cryptocurrency tracing, dark web, money laundering, cybercrime.

I. INTRODUCTION

The swift development of blockchain technology and cryptocurrencies has revolutionized global finance, presenting both extraordinary potential and unparalleled challenges. The decentralized and transparent characteristics of blockchain have promoted financial inclusion, lowered transaction expenses, and allowed for rapid, safe international transfers (Meiklejohn, *et al*. 2013; Reid and Harrigan 2013). This innovation has transformed conventional financial institutions, providing individuals and enterprises an alternative to centralized banking frameworks. Nonetheless, the very attributes that render blockchain a formidable financial instrument have also posed considerable obstacles, especially in the field of criminology. The anonymous characteristics of blockchain transactions, along with its worldwide accessibility and absence of centralized oversight, have enabled unlawful financial operations on an unparalleled scale.

A significant risk regarding bitcoin adoption is its involvement in cybercrimes, such as money laundering, ransomware attacks, fraud, and illegal transactions on dark web marketplaces. The capacity to transfer substantial amounts of money internationally without intermediaries has drawn the attention of cyber-criminals, allowing them to circumvent conventional financial oversight. The dark web has emerged as a nexus for unlawful activity (Foley, *et al*. 2019), where offenders utilize cryptocurrency to exchange contraband, perpetrate fraud schemes, and finance organized crime enterprises. Ransomware assaults have increased, with fraudsters requesting payments in cryptocurrencies (Moser *et al*. 2013) to avoid detection by law authorities (Campisi and Celeste, 2021). The decentralized characteristic of cryptocurrencies has rendered it difficult for authorities to control transactions efficiently, underscoring the necessity for sophisticated forensic methodologies (Gai, *et al*. 2021; Huang and Saxena, 2019).

Cryptocurrencies, especially Bitcoin, were once seen as anonymous because of the pseudonymous characteristics of wallet addresses (Möser, *et al*. 2018). Nonetheless, advancements in blockchain analytics have shown that transactions documented on public ledgers are traceable, allowing authorities to de-anonymize unlawful operations. Although Bitcoin is the predominant cryptocurrency utilized for unlawful transactions, privacy-centric cryptocurrencies like Monero and Zcash have surged in favor among criminals owing to their superior anonymity attributes (Möser, *et al*. 2018). These privacy coins employ cryptographic methods like ring signatures and stealth addresses, complicating forensic investigations. As cybercriminals employ increasingly sophisticated techniques to conceal their transactions, law enforcement organizations must perpetually advance their forensic methodologies to be effective.

[*] Address correspondence to this author at the Brainster Next College, Skopje, North Macedonia; E-mail: jelena.gjorgjev1@gmail.com

Blockchain forensic technologies like Chainalysis, CipherTrace, and Elliptic have been instrumental in significant investigations, resulting in the disbandment of criminal organizations and the retrieval of illicit assets. These technologies utilize sophisticated algorithms to monitor cryptocurrency transactions, analyze blockchain data, and detect anomalous trends. Prominent instances, including the dismantling of the Silk Road bazaar and the tracking of Colonial Pipeline ransomware payments, underscore the changing dynamics of blockchain-facilitated crime and corresponding countermeasures. Blockchain analytics has become indispensable in criminal investigations, equipping law enforcement authorities with the requisite tools to address financial crimes in the digital era.

This paper seeks to examine the convergence of blockchain technology and criminology, concentrating on the techniques utilized in blockchain forensic investigations. This will analyze essential methodologies including clustering analysis, transaction graph mapping, and heuristic strategies employed to track illicit cryptocurrency transactions. These approaches have demonstrated efficacy in revealing criminal actions, enabling investigators to associate digital assets with real-world identities. The paper will examine the legal, ethical, and regulatory ramifications of blockchain forensics, focusing on the delicate equilibrium between privacy rights and criminal deterrence (A. Zohar, 2015). As governments and regulatory entities endeavor to establish frameworks for cryptocurrency regulation, the conflict between financial privacy and law enforcement surveillance persists as a significant discourse.

This paper will analyze real-world case studies to assess the efficacy of blockchain forensic approaches and suggest future strategies for addressing cryptocurrency-related crimes. The paper will evaluate the limitations of existing forensic tools and examine prospective technology developments that may improve the efficacy of blockchain investigations. With the increasing popularity of cryptocurrencies, the demand for effective forensic methodologies and global collaboration in the prevention of financial crimes will become increasingly urgent. The findings of this paper will contribute to the ongoing discourse on the role of blockchain in financial crime, offering practical recommendations for policymakers, forensic analysts, and law enforcement agencies to navigate the complexities of cryptocurrency-related investigations.

II. LITERATURE REVIEW

Blockchain forensics has become an essential domain in digital investigations, integrating aspects of conventional digital forensics with sophisticated blockchain analytics.

Atlam and Wills (Atlam and Wills, 2023) performed a thorough literature assessment of 46 papers to identify digital forensic frameworks and approaches employed in blockchain forensics, emphasizing the strengths and limits of the subject.

Filipov and Bilić (Filipov and Bilić, 2023) developed a systematic methodology for examining financial crimes with blockchain technology, highlighting data gathering, preservation, processing, and presentation as essential elements of successful investigations.

(Dasaklis, *et al*. 2020) presented a comprehensive analysis and categorization of blockchain-based digital forensic tools, analyzing the advantages and obstacles of incorporating blockchain technology into established forensic practices.

(Osterrieder, *et al*. 2025) examined irregularities and fraud in blockchain networks, providing insights on detection and prevention methodologies via machine learning, digital forensics, and risk assessment tools.

(Bonomi, *et al*. 2018) developed a blockchain-based chain of custody paradigm for digital forensics, demonstrating the capability of blockchain technology to improve the integrity and traceability of digital evidence.

These studies together enhance the comprehension of blockchain forensics by examining diverse approaches, frameworks, and applications, hence improving the efficacy of forensic investigations within blockchain contexts.

A. The Dark Web and Cryptocurrency Crime

The dark web has emerged as a primary marketplace for illegal operations, with bitcoins serving a vital function in enabling these transactions. Online black markets like Silk Road, Hydra, and AlphaBay illustrate how cryptocurrency facilitate anonymous transactions for illicit products and services, including narcotics, firearms, and forged documents. In contrast to conventional banking systems that necessitate identification verification and adherence to regulations, dark web marketplaces function within a predominantly unregulated environment, where transactions are conducted anonymously via bitcoin payments. Bitcoin served as the principal medium of trade for these networks owing to its pseudonymous characteristics; but, with the advancement of forensic tools, criminals begun transitioning to privacy-centric cryptocurrencies such as Monero, which conceals transaction information.

Cryptocurrencies are significantly implicated in human trafficking, as traffickers utilize digital assets to accept money while preserving anonymity. The decentralized structure of blockchain networks hinders authorities' ability to oversee transactions, hence complicating the tracking and dismantling of illegal networks. Moreover, ransomware incidents have surged in recent years, with perpetrators demanding bitcoin payments for the decryption of compromised computers. The Colonial Pipeline attack exemplifies the escalating threat from ransomware gangs who leverage blockchain anonymity to extort corporations and individuals.

B. Blockchain’s Transparent Yet Pseudonymous Nature

A notable paradox in blockchain technology is its integration of transparency and pseudonymity. All Bitcoin and Ethereum transactions are documented on a public ledger, rendering it theoretically feasible to track financial transactions. Nonetheless, the names of wallet holders remain obscured until associated with an external institution, such as a centralized exchange that mandates Know Your Customer (KYC) compliance. Criminals utilize this characteristic by employing several wallets, coin mixers, and decentralized exchanges to conceal their identity.

Law enforcement organizations encounter difficulties in monitoring offenders using blockchain networks because of the absence of direct identity connections. Although addresses and transaction information are publicly available, linking wallets to persons necessitates advanced forensic methods. Criminals frequently utilize transaction obfuscation technologies like tumblers and private wallets, complicating investigators' efforts to establish clear links between transactions and criminal entities.

C. Forensic Blockchain Techniques

A variety of forensic methodologies have been established to monitor illegal blockchain transactions.

- Clustering Analysis: This method categorizes associated addresses managed by a singular entity. Through the analysis of transaction patterns, forensic investigators can connect many wallets linked to criminal activity, allowing police to reveal extensive unlawful networks.

- Heuristic Techniques: These strategies discern wallet ownership patterns utilizing established behavioral cues. Wallets that often engage with illicit services on the dark web may be designated as high-risk, enabling authorities to more efficiently monitor dubious transactions.

- Address Tagging: Law enforcement organizations and blockchain analytics firms curate lists of banned addresses associated with illicit operations. Through the cross-referencing of transaction histories, investigators can trace illicit payments to their origins, facilitating the identification and punishment of perpetrators.

- Transaction Graph Analysis: This technique delineates the movement of funds within the blockchain, revealing patterns suggestive of money laundering or unlawful financial operations. By visualizing cryptocurrency transactions, investigators can trace the flow of illicit funds across several wallets and exchanges, aiding in the identification of principal actors in criminal enterprises.

These forensic tools have been essential in significant criminal investigations, enabling law enforcement agencies to track illicit bitcoin transactions and dismantle criminal networks. As criminals employ increasingly sophisticated evasion strategies, forensic procedures must evolve to counteract rising dangers.

III. METHODOLOGY

This paper utilizes a complete methodological approach that combines qualitative and quantitative research approaches, based on the frameworks established by (Yin 2018; Creswell, 2014). The extensive methodological framework is defined by the amalgamation of forensic data analysis, legal assessments, and expert opinions, offering a multifaceted view on blockchain forensic methodologies.

A. Forensic Data Examination

Blockchain forensic investigations utilize data analytic methodologies to trace cryptocurrency movements and detect unlawful activities. This paper investigates transaction clustering methodologies, machine learning-based anomaly detection, and address attribution approaches. Data from cryptocurrency forensic organizations like Chainalysis and CipherTrace is utilized to evaluate how blockchain analytics technologies detect anomalous transaction patterns and trace unlawful financial activity.

B. Examination of Legal and Regulatory Framework

Regulatory frameworks are essential in influencing blockchain forensic methods. This paper evaluates national and international rules, encompassing anti-money laundering (AML) and counter-terrorism financing (CTF) policies, to determine their influence on blockchain investigations. Legal documents, governmental rules, and compliance reports are scrutinized to assess the efficacy of regulatory measures in preventing financial crimes associated with cryptocurrencies.

C. Expert Interviews and Case Evaluations

This paper integrates expert interviews with forensic analysts, cybersecurity specialists, and law enforcement personnel engaged in cryptocurrency investigations to achieve a realistic understanding of blockchain forensics. Case reviews offer insights into the practical applications of forensic techniques, emphasizing effective interventions and pinpointing difficulties in monitoring illicit blockchain transactions.

D. Ethical Considerations

Although blockchain forensics is crucial in addressing financial crimes, it presents ethical dilemmas related to privacy and surveillance. The efficacy of forensic techniques in monitoring bitcoin transactions must be balanced with people' rights to financial privacy. This paper rigorously analyzes the ethical ramifications of blockchain surveillance, assessing the equilibrium between crime deterrence and civil freedoms. Discussions encompass the dangers of governmental overreach, the exploitation of forensic technologies, and the effects of heightened surveillance on genuine bitcoin users.

This methodology offers a comprehensive framework for assessing blockchain forensic methodologies through the integration of forensic data analysis, legal evaluations, and expert perspectives. This paper will provide significant recommendations for improving the efficacy of blockchain forensic investigations while maintaining ethical and legal adherence.

IV. CASE STUDIES

This section's case studies illustrate the practical implementation of the blockchain forensic approaches previously mentioned. This section seeks to correlate theoretical techniques with empirical facts by examining real-world cases, including the Silk Road investigation, the Bitfinex breach, and the Colonial Pipeline ransomware assault. Each case study is carefully selected to demonstrate particular forensic techniques, including transaction clustering, address attribution, and machine learning-based anomaly identification. This study demonstrates how blockchain forensics can proficiently track illicit transactions, assist law enforcement efforts, and tackle the emerging issues of financial crime in digital contexts. These case cases not only corroborate the forensic approaches examined but also elucidate the constraints and prospects for future developments in blockchain analytics.

A. The Silk Road Inquiry

Silk Road was an infamous dark web bazaar that enabled illegal transactions utilizing Bitcoin. Law enforcement agencies effectively employed blockchain forensic methods to trace Bitcoin transactions, leading to the identification and arrest of its founder, Ross Ulbricht (Cracking the Silk Road & Capturing Darknet's DPR). Investigators employed transaction clustering analysis and address attribution to trace payments on the platform, uncovering connections between Silk Road administrators and illicit operations. This case represented a major achievement in illustrating the efficacy of blockchain forensics in combating cybercrime (Lessons Learned from the Silk Road Investigation).

B. The Bitfinex Breach

The 2016 Bitfinex breach led to the appropriation of 119,756 Bitcoin (Bitfinex Hack Money Launderers Plead Guilty). For numerous years, law enforcement agencies monitored these monies as they traversed multiple wallets and mixers. Employing blockchain forensic methodologies, including heuristic transaction tracing and machine learning anomaly detection, authorities successfully identified the hackers and reclaimed a substantial percentage of the misappropriated assets (The US$4.5 Billion Bitfinex Hack – Five Things You Should Know). This case underscores the difficulties associated with cryptocurrency laundering and the advancing proficiency of blockchain forensics.

C. Ransomware Attack on Colonial Pipeline

In 2021, Colonial Pipeline experienced a ransomware assault resulting in a payment of $4.4 million in Bitcoin. Law enforcement officials effectively traced and retrieved a significant chunk of the ransom through blockchain research (Colonial Pipeline Ransomware Attack: What Happened?). This case illustrated the efficacy of forensic transaction analysis in countering ransomware activities and retrieving illegal monies, establishing a benchmark for subsequent inquiries into cryptocurrency-related cybercrimes (B. Smith).

V. FINDINGS AND DISCUSSION

This part consolidates the findings from the previously published case studies and theoretical analysis. The results underscore the efficacy of blockchain forensic techniques in practical applications, illustrating success in the identification and prosecution of fraudsters via comprehensive forensic procedures.

A. Efficacy of Blockchain Forensic Methodologies

The paper demonstrates that blockchain forensic techniques, such as clustering analysis, transaction graph mapping, and heuristic analysis, are effective in identifying illicit activities on the dark web (Meiklejohn, *et al*. 2013). These approaches have enabled the identification of criminals engaged in money laundering, drug trafficking, and ransomware assaults (Reid and Harrigan 2013) by de-anonymizing blockchain transactions and supplying tangible proof for legal punishment (Conti *et al*. 2018).

B. Clustering Analysis in Deconstructing Illicit Networks

Clustering research has been quite helpful in delineating intricate criminal networks. Through the analysis of transaction patterns and the identification of clusters of wallets linked to illicit operations, law enforcement organizations can reveal concealed relationships among cybercriminals. The Silk Road case study illustrates how clustering analysis facilitated the identification of transactions linked to the platform's founder, Ross Ulbricht, culminating in his apprehension (Cracking the Silk Road & Capturing Darknet's DPR; Lessons Learned from the Silk Road Investigation).

C. Forecasting High-Risk Wallets using Heuristic Methods

The paper highlights the effectiveness of heuristic methods in forecasting high-risk cryptocurrency wallets. These strategies employ behavioral patterns and transactional data to identify wallets potentially engaged in illicit activity. This predictive ability improves proactive oversight and facilitates swifter intervention by authorities.

D. Reconciling Transparency and Financial Privacy

A key problem identified is achieving a balance between investigative transparency and safeguarding genuine financial privacy. The results demonstrate that although blockchain analytics tools are effective in tracking illicit transactions, there exists a risk of encroaching upon legitimate financial activity if not adequately regulated.

E. Adjustment to Developing Cybercriminal Strategies

As fraudsters employ increasingly complex techniques, including the utilization of privacy-focused cryptocurrencies like Monero and the exploitation of decentralized exchanges, law enforcement authorities must therefore adjust their strategies. The paper underscores the necessity for ongoing enhancement of forensic instruments and global cooperation to successfully tackle these advancing challenges.

VI. CHALLENGES AND LIMITATIONS

Although blockchain forensics has markedly improved law enforcement's capacity to trace unlawful bitcoin transactions, numerous obstacles and limits persist. Criminals consistently modify their strategies in response to advancing forensic methodologies, employing privacy-enhancing technologies and decentralized networks to avoid discovery. Forensic investigators have several significant hurdles when tracing unlawful blockchain transactions (Möser, *et al*. 2013; Campisi and Celeste, 2021).

A. Emergence of Privacy Coins

Privacy-centric cryptocurrencies like Monero, Zcash, and Dash have posed considerable challenges for forensic examination (Möser, *et al*. 2018). In contrast to Bitcoin, which utilizes a public ledger for transaction tracing, privacy coins employ cryptographic methods such as ring signatures, stealth addresses, and zero-knowledge proofs to conceal transaction information. Monero, for instance, amalgamates numerous transactions into a singular input, rendering it very hard to ascertain the sender or recipient. Zcash, via its shielded transactions, encrypts all data pertaining to the sender, receiver, and transaction amount, hence exacerbating forensic challenges.

Furthermore, offenders utilize bitcoin mixers, including Tornado Cash and Blender.io, to obscure their transaction records. Mixers sever the connection between senders and recipients by aggregating funds from numerous users and redistributing them in minimal quantities, hence undermining conventional forensic tracing methods. Law enforcement agencies are persistently advancing countermeasures to address these issues; nonetheless, privacy-enhancing characteristics of cryptocurrencies significantly impede forensic investigations.

B. Decentralized Exchanges and Unregulated Platforms

Decentralized exchanges (DEXs) function autonomously, enabling users to trade cryptocurrencies straight from their wallets without the necessity of identification verification. In contrast to centralized exchanges that implement Know Your Customer (KYC) and Anti-Money Laundering (AML) rules, decentralized exchanges (DEXs) offer total anonymity, rendering them appealing to criminals aiming to launder illicit funds. The absence of regulatory control on these platforms obstructs law enforcement initiatives, as there is no centralized authority to subpoena transaction records.

The emergence of DeFi (Decentralized Finance) systems has exacerbated the complexity of forensic investigations. Smart contracts enable peer-to-peer transactions, lending, and borrowing devoid of intermediaries, hence generating new vulnerabilities that criminals use for unlawful financial activity. DeFi protocols facilitate flash loan attacks, wash trading, and rug pulls, exacerbating the challenges encountered by forensic investigators in monitoring and tracing fraudulent transactions.

C. Legal and Ethical Issues

The most contentious feature of blockchain forensic investigations is the equilibrium between crime deterrence and financial privacy. Law enforcement organizations contend that forensic tracing is essential for combating unlawful activity, whereas privacy advocates express worries regarding mass surveillance and the potential misuse of forensic techniques. Blockchain transactions were originally intended to provide financial autonomy and pseudonymity, and excessive forensic examination could undermine these essential concepts.

Moreover, legal frameworks governing blockchain forensics differ internationally, with many jurisdictions enforcing stringent privacy regulations that restrict forensic data acquisition. The absence of global cooperation in regulating cryptocurrency tracking complicates law enforcement authorities' ability to conduct effective cross-border investigations. Variations in legal interpretations and regulatory deficiencies enable criminals to exploit states with lax enforcement, hindering global initiatives to address blockchain-related financial crimes.

As blockchain technology advances, law enforcement agencies and forensic specialists must confront these problems by creating more advanced forensic tools, improving regulatory collaboration, and assuring ethical adherence in forensic investigations. The future of blockchain forensics depends on achieving a balance between security and privacy while reacting to emerging technical advancements that transform the financial landscape.

VII. CONCLUSION AND POLICY RECOMMENDATIONS

The evolution of blockchain technology raises substantial concerns regarding its influence on financial security and crime prevention. Although blockchain forensics has significantly advanced in monitoring and countering illegal cryptocurrency operations, continuous enhancements are essential to match the developing strategies of hackers. This section delineates future ideas for improving blockchain forensic methodologies, achieving equilibrium between financial privacy and crime deterrence, and formulating more robust legislative frameworks to assist law enforcement agencies.

A. Advancements in Blockchain Forensic Methodologies

Continuous developments in forensic tools are required to effectively tackle cryptocurrency-related crimes. Machine learning and artificial intelligence (AI) are essential for enhancing the precision of transaction pattern detection (Dasaklis, *et al*. 2020), detecting anomalous behavior, and forecasting fraudulent operations in real-time (Osterrieder, *et al*., 2024). Creating sophisticated blockchain analytics tools that incorporate AI-driven anomaly detection can greatly improve forensic capabilities.

A significant enhancement pertains to the augmentation of cross-chain analysis. Criminals often utilize various blockchain networks to launder money, necessitating the development of forensic systems capable of efficiently tracking transactions across multiple chains. Improving interoperability among blockchain forensic platforms and creating multi-chain analysis tools will furnish investigators with a more holistic perspective on illegal activity.

Moreover, forensic specialists must enhance transaction de-anonymization methodologies for privacy cryptocurrencies like Monero and Zcash. Although these cryptocurrencies present considerable obstacles for law enforcement, investigating statistical analysis and heuristic approaches may facilitate the identification of concealed transaction patterns, hence enhancing traceability.

B. Achieving Equilibrium between Financial Confidentiality and Criminal Deterrence

A significant problem in blockchain forensics is reconciling financial privacy with the necessity of crime prevention. Although law enforcement organizations necessitate access to transaction data for criminal investigations, excessive surveillance may jeopardize individual financial liberties. Policymakers must guarantee that forensic techniques are employed properly and in compliance with legal standards to avert overreach.

A possible strategy is the adoption of privacy-preserving forensic solutions. Zero-knowledge proofs and cryptographic auditing methods allow law enforcement authorities to authenticate transaction validity while safeguarding sensitive user information (Bonomi, *et al*. 2018). These privacy-preserving technologies would enhance transparency while protecting individual rights.

Moreover, interactions between regulatory authorities, blockchain developers, and forensic organizations can enhance ethical crime prevention strategies. Promoting the incorporation of compliance tools, such as opt-in transparency features, into blockchain networks helps reconcile the conflict between privacy and law enforcement requirements.

C. Enhancing Regulatory Frameworks to Bolster Law Enforcement Agencies

To improve the efficacy of blockchain forensics, regulatory bodies must implement more rigorous supervision of cryptocurrency exchanges, decentralized finance (DeFi) platforms, and privacy-enhancing technology. Enforcing obligatory Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements for all bitcoin service providers will diminish the capacity of criminals to exploit the anonymity inherent in blockchain networks.

Global collaboration is essential in combating blockchain-related criminal activities. Cybercriminals frequently function across several jurisdictions, necessitating the establishment of worldwide regulatory standards by governments. Collaborative initiatives, like information-sharing agreements among law enforcement agencies and the establishment of multinational task teams focused on blockchain forensic investigations, can enhance cross-border crime prevention.

In conclusion, although blockchain technology presents both benefits and problems, proactive actions can effectively limit its hazards. By improving forensic methodologies, maintaining ethical privacy standards, and reinforcing regulatory structures, authorities may guarantee that blockchain continues to serve as a secure and transparent financial instrument while reducing its potential for criminal exploitation.

REFERENCES

A. Zohar, “Bitcoin: Under the Hood,” Communications of the ACM, vol. 58, no. 9, pp. 104–113, 2015. https://doi.org/10.1145/2701411

B. Smith, “FBI Recovers Colonial Pipeline Ransom Payment,” BBC News. (Online). Available: https://www.bbc.com/news/technology-57399493.

“Bitfinex Hack Money Launderers Plead Guilty,” Chainalysis. (Online). Available: https://www.chainalysis.com/blog/bitfinex-hack-plea-july-2023.

“Colonial Pipeline Ransomware Attack: What Happened?” CISA. (Online). Available: https://www.cisa.gov/news-events/cybersecurity/colonial-pipeline-ransomware-attack.

“Cracking the Silk Road & Capturing Darknet's DPR,” Forensics Colleges. (Online). Available: https://www.forensicscolleges.com/blog/forensics-casefile/silk-road.

F. Reid and M. Harrigan, “An Analysis of Anonymity in the Bitcoin System,” in Security and Privacy in Social Networks, Springer, 2013, pp. 197–223. https://doi.org/10.1007/978-1-4614-4139-7_10

G. Gai, C. Jiang, S. Guo, and Y. Qian, “Blockchain and Smart Contract for IoT-Based Applications: A Survey,” IEEE Internet of Things Journal, vol. 8, no. 2, pp. 1371–1392, 2021. https://doi.org/10.1109/JIOT.2020.3036705

J. Möser, R. Böhme, and D. Breuker, “An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem,” APWG eCrime Researchers Summit, 2013. https://doi.org/10.1109/eCRS.2013.6805780

J. Osterrieder, S. Lokhov, and T. Shams, “Detecting Anomalies and Frauds in Blockchain Networks,” arXiv preprint arXiv:2402.11231, 2024. (Online). Available: https://arxiv.org/abs/2402.11231.

J. W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 4th ed., SAGE Publications, 2014.

“Lessons Learned from the Silk Road Investigation,” Belkasoft. (Online). Available: https://belkasoft.com/silk-road-investigation-lessons-learned.

M. Atlam and G. Wills, “Blockchain Forensics: A Systematic Literature Review,” Electronics, vol. 13, no. 17, 2023. https://doi.org/10.3390/electronics13173568

M. Conti, S. Kumar, C. Lal, and S. Ruj, “A Survey on Security and Privacy Issues of Bitcoin,” IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018. https://doi.org/10.1109/COMST.2018.2842460

M. Möser, K. Soska, E. Heilman, K. Lee, H. Narula, and N. Christin, “An Empirical Analysis of Traceability in the Monero Blockchain,” Privacy Enhancing Technologies Symposium, vol. 2018, no. 3, pp. 143–163. https://doi.org/10.1515/popets-2018-0025

P. Campisi and C. Celeste, “Cryptocurrency Mixing Services: Analysis and Detection,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2089–2102, 2021.

P. Dasaklis, N. Casino, and C. Patsakis, “Blockchain-based digital forensic tools: A classification and research outlook,” arXiv preprint arXiv:2005.12640, 2020. (Online). Available: https://arxiv.org/abs/2005.12640.

R. K. Yin, Case Study Research and Applications: Design and Methods, 6th ed., SAGE Publications, 2018.

S. Bonomi, R. Di Pietro, and F. Martinelli, “B-CoC: A Blockchain-Based Chain of Custody for Digital Forensics,” arXiv preprint arXiv:1807.10359, 2018. (Online). Available: https://arxiv.org/abs/1807.10359.

S. Foley, J. R. Karlsen, and T. J. Putniņš, “Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?,” Review of Financial Studies, vol. 32, no. 5, pp. 1798–1853, 2019. https://doi.org/10.1093/rfs/hhz015

S. Meiklejohn, M. Pomarole, G. Jordan, *et al*., “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names,” Proc. ACM Internet Meas. Conf., 2013, pp. 127–140. https://doi.org/10.1145/2504730.2504747

T. Y. K. Huang and P. Saxena, “A Closer Look at Bitcoin Mining Pools: Security and Privacy Implications,” Proc. IEEE Symposium on Security and Privacy Workshops (SPW), 2019, pp. 451–466.

“The US$4.5 Billion Bitfinex Hack – Five Things You Should Know,” Hogan Lovells. (Online). Available: https://www.hoganlovells.com/en/publications/the-us45-billion-bitfinex-hack-five-things-you-should-know.

V. Filipov and V. Bilić, “A Modern Approach to Investigating Financial Crimes Using Blockchain Forensics,” ResearchGate, 2023. (Online). Available: https://www.researchgate.net/publication/368910848_Blockchain_Forensics.

Received on 09-01-2025 Accepted on 06-02-2025 Published on 04-03-2025

https://doi.org/10.6000/1929-4409.2025.14.07