# Blockchain Forensics in Dark Web Investigations: A Comprehensive Review of Techniques, Challenges

*Boora Swagath[1*], Bhukya Veerender Sehwag[2], Venna Shivamani[3], Vinod Kaaparthi[4].*
*[1*,2,3]B.Sc. (Hons) Digital Forensic Science, Malla Reddy University, Hyderabad, India*
*[4]Assistant Professor, Department of Digital Forensic Science, Malla Reddy University, Hyderabad, India*
*[*]swagathbura06@gmail.com*

## Abstract

The dark web has emerged as the center of several online crimes in recent times such as distribution of illegal drugs, ransomware, human trafficking, and financial crimes. In order to carry out such crimes, the dark web markets tend to utilize cryptocurrency, because it is decentralized and has the perceived neutrality. The technology behind the cryptocurrencies, the Blockchain is however Baffling by Nature. Given that the technology of cryptocurrencies is the Blockchain, and cryptocurrencies are deemed to be anonymous, these appear to be a paradox as the Blockchain is transparent and non-editable, which makes all the transactions recorded even more traceable. However, the traceability costs are miraculously reduced since all the transactions are recorded, and the users of the technology generate "pseudonyms" of the transactions. Digital forensic science exploits this paradox. This paper reviews the application of Blockchain technology in the investigation of the dark web and the increasing importance of Blockchain technology in the current policing environment. This paper reviews current literature around Blockchain technology and digital forensic techniques, including transaction analysis techniques, address clustering, network mapping, and digital forensic attribution techniques. This paper further describes the role of advanced Blockchain analytical platforms in the identification of suspicious transaction patterns and the tracking of these patterns back to real-world entities. Furthermore, the challenges being currently faced during the investigation of Blockchain technology, including the usage of privacy coins, mixing services, and cross-train transactions, that increase the difficulties of these investigations, have also been considered. This paper, thus, clearly supports the premise that the current investigation challenges notwithstanding, Blockchain technology can clearly serve the needs of the digital forensic investigation of the dark web and that the importance of Blockchain technology is only increasing.

**Keywords:** Dark Web, Cryptocurrency Forensics, Blockchain Technologies, Pseudonymous Transactions, Artificial Intelligence in Forensics, Cybercrime Investigation, Network Mapping.

© The Author(s) 2026
D. R. Reddy et al. (eds.), *Proceedings of the First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)*, Advances in Computer Science Research 127,
https://doi.org/10.2991/978-94-6239-610-4_21

## 1. Introduction

The swift growth of internet technologies has led to the growth of the deep web and the dark web bringing new opportunities and challenges to cybersecurity and law enforcement. Dark web is a hidden part of the net that is deliberately covered and may only be accessed with the use of anonymization services like The Onion Router (Tor). Although these technologies were initially created with the goal of safeguarding privacy and facilitating freedom of expression, they have also been used more and more to conduct illegal actions such as hacking services, ransomware attacks, illicit drug trade, financial fraud, identity theft, and human trafficking (Al-Nemrat et al., 2020).

The use of cryptocurrencies as the main form of exchange is a specific feature of the dark web marketplaces. Bitcoin and other cryptocurrencies are decentralized, borderless, requiring no conventional financial intermediary, which includes them in the portfolio of cybercriminals (Nakamoto, 2008). The initial views of cryptocurrencies were those of fully anonymous system but later studies have shown that most cryptocurrencies based on blockchain technology are actually pseudonymous but not completely anonymous (Reid and Harrigan, 2013). Any transaction performed in any public blockchain is a set of permanent records on distributed ledgers, which permits investigators to examine transaction histories in a retrospective manner.

This natural transparency has made it possible to develop blockchain forensics as a field, which is concerned with deriving investigative intelligence off blockchain information. Blockchain forensics enables investigators to track illegal currency movements, discover fund escrow accounts at the start and finish of marketplaces, and connect on-chain evidence with off-chain trustworthy data by utilizing methods like analysis of transaction graphs, clustering addresses, and attributing entities (Meiklejohn et al., 2013). Such methods have been instrumental in major dark web crackdowns, such as the takedowns of Silk Road, AlphaBay and Hansa marketplaces.

Simultaneously, the ever-increasing amount and sophistication of blockchain and dark web data have made it necessary to adopt machine learning and artificial intelligence methods. These strategies assist in automated detection of anomalies, categorization of malicious activity, and scalable transactions analysis, which allow investigators to manipulate very large datasets that could not be dealt with, the traditional rule-based forensic approach (Yadav and Singh, 2022). These technologies have ethical, legal and governance challenges associated with privacy, explainability, and admissibility of evidence despite its benefits.

Despite the great research on the topic of dark web ecosystems, blockchain forensics, and AI-based investigation methods, the literature is still disjointed across disciplines. The necessity to thoroughly examine the areas is evident and integrate them to determine their overall impact on detecting and analyzing dark marketplaces. The present paper fills this gap by conducting a systematic review of literature on blockchain forensics in investigations of dark web, identifying the existing capabilities and limitations, and discussing the future research perspectives.

## 2. Literature Review

The initial research on the dark web was mainly aimed at the organization of underground markets, their economy, and social life. The Silk Road marketplace was one of the most powerful studies that showed how the cryptocurrencies were used to engage in large-scale illicit trade, but at the same time capture all the transactions on a publicly available blockchain (Christin, 2013). This publication disrupted the fact that the assumption of cryptocurrency-based payments being completely anonymous and unreliable was supported.

The follow-up studies were replaced with the examination of the forensic capability of blockchain systems. The works of Meiklejohn et al. (2013) and Reid and Harrigan (2013) revealed that transaction graph modeling and the address clustering heuristic might be used to correlate several wallet addresses with one controlling entity. Through the analysis of common inputs in transactions, time associations and recurrent spending patterns, scientists developed frameworks that remain the basis of contemporary blockchain forensic studies.

The degree of criminalization that is enabled by cryptocurrencies has also been measured quantitatively. Foley et al. (2019) estimated that a good part of Bitcoin transactions was linked to illegal activities such as dark Web markets and financial offenses. These results supported the significance of blockchain analytics as a fundamental investigation instrument in the enforcement of cybercrime. Further research also highlighted the importance of integrating on-chain blockchain data with off-chain intelligence sources, i.e., with servers seized, cryptocurrency exchange data, and Know Your Customer (KYC) data, to enhance attribution and the reliability of the evidence (Moser et al., 2013).

Machine learning algorithms have been used to differentiate between benign and malicious transactions and wallet addresses with supervised learning models, and unsupervised artificial intelligence algorithms like clustering and anomaly detection have been applied to discover criminal behavior previously unknown (Vaghela et al., 2025). Later studies have also proposed new graph based learning models, such as graph neural networks, to provide more intricate transactional relationships in blockchain ecosystems (Osterrieder et al., 2024).

Nevertheless, in spite of these developments, the literature continues to emphasize the issues that are still a challenge. Cryptocurrencies that improve privacy, coin-mixing services, decentralized exchanges, and cross-chain transactions contribute greatly to the overall lack of traceability of transactions and attack conventional forensic heuristics (Campisi and Celeste, 2021). Moreover, the problem of legal and ethical limitations to using real-world dark web datasets makes the use of simulated or partially labeled data very common. Surveillance-related ethical issues, privacy invasion, and the legal admissibility of blockchain evidence are also becoming more prominent in the recent research (Europol, 2023).

In general, the literature confirms blockchain forensics as a vital element of contemporary dark web investigations and at the same time exposes technical, legal, and ethical issues that have not been resolved yet. These results have highlighted the importance of combining adaptable and integrated forensic frameworks that integrate machine learning, blockchain analytics and conventional digital forensics. This review is a continuation of the previous studies that combine all these areas to establish existing trends, gaps in research and prospects of effective investigation of the dark web.

## 3. Background and Related Work

### 3.1 Dark Web Ecosystem and Cybercrime

The dark web is a hidden part of the internet that is based on anonymizing technologies like The Onion Router (Tor) that hides user identities and IP address by directing traffic over a series of encrypted nodes. Even though services were created with the intention of safeguarding privacy and freedom of expression, they have over the years been abused by criminals (Al-Nemrat et al., 2020). Consequently, the dark web has been transformed into a platform of cyber-facilitated criminal activities such as drug trafficking, ransomware distribution, identity theft, financial fraud, and sale of weapons and human trafficking.

Dark web markets are decentralized networks in which sellers and buyers exchange messages and most transaction is typically conducted with cryptocurrency as the main medium of

exchange. These markets tend to use escrow services, reputation system and encrypted communication channels to allow trust among participants and reduce the risks of being exposed (Christin, 2013). These platforms are decentralized and transnational, and this presents great challenges to traditional methods of law enforcement that are power based on the jurisdictions and centralized infrastructure.

According to the studies on bibliometrical and trend analysis, it can be stated that the academic research on the topic of dark web cybercrime grows steadily over the ten years. The primary themes of research mentioned in the current literature are the recognition of cybercrime patterns, the analysis of the underground economy, the distribution of malware, and the extraction of threat intelligence (Al-Nemrat et al., 2020). In addition to the cybersecurity implication, more recent research studies highlight the implications of the dark web activities on society as a whole, such as the role of the activities in endangering the health of the population due to drug trafficking, to the national security, as well as the issues of digital governance (Europol, 2023; UNODC, 2022). These results emphasize the need to conduct interdisciplinary studies on the nature of dark web-enabled crime and measures to mitigate it.

**3.2 Dark Web Analysis by machine learning and artificial intelligence.**

The high-volume, dynamic and anonymized character of the dark web information poses a significant challenge to the productivity of conventional digital forensic techniques. The most typical methods of tracing IP addresses, packet inspection, and traditional content analysis usually cannot work because of the extensive use of encryption, onion routing, and techniques of obfuscation (Conti et al., 2018). Therefore, the use of machine learning (ML) and artificial intelligence (AI) methods to improve the investigative power in dark web contexts has gained popularity among researchers.

Controlled machine learning models, such as Support Vector Machines and Random Forest classifiers, and neural networks, have been used to identify suspicious activity, categorize illicit marketplace listings, and determine malicious actors through the application of behavioural and transactions features (Yadav and Singh, 2022). Simultaneously, unsupervised and semi-supervised methods like clustering, topic model and anomaly detection have been employed to reveal previously unknown patterns of crime without subject to labeled training data.

Besides content-based analysis, there are also network traffic fingerprinting and flow analysis methods to determine the user behavior without decrypting traffic and thus maintain data integrity but provide insight into the investigation (Vaghela et al., 2025). Those methods examine the timing, packet sizes, and frequency of communication with the dark web to determine the correlations between dark web usage and illegal activity.

Although effective, the application of AI surveillance tools elicits significant issues of data validity, generalizability of the model, explainability, and ethical applications. A number of reports warn that subjective training statistics, black box decisions, and over-spying can erode trust in the outcomes of forensic investigations and create legislative issues on the use of evidence in the courtroom (Conti et al., 2018). Such constraints indicate that explainable, ethically controlled AI systems are required in the research of the dark web.

**3.3 Blockchain Technology and Cryptocurrency forensics.**

Most dark web market places rely on cryptocurrencies as the financial backbone because of their decentralized structure, censorship resistance and their facilitation of cross-border payments. Pioneering views and impressions have considered cryptocurrencies as a completely anonymous payment system but it has since been revealed that most open blockchain networks are not anonymous but only pseudonymous (Reid and Harrigan, 2013).

Bitcoin and Ethereum are examples of public blockchains that have transparent and unchanging

registries that permanently store all transactions. Through this transparency, forensic investigators are able to perform transaction history analysis through the application of address clustering techniques, heuristic-based linkage analysis techniques, and transaction graph modeling techniques (Meiklejohn et al., 2013). These techniques can enable investigators to allot more than one set of wallet addresses to one person and follow a trail of illegal money through complicated transaction networks.

Numerous practical studies have shown the practicability of blockchain analytics with respect to the process of tracking revenues and ransomware payments on the dark web marketplaces, as well as mass theft of cryptocurrencies. Research has shown that although criminals may seek to obscure a transaction through mixing services or wallets, behavior and interactions with regulated exchanges can still be used to attribute any transaction (Moser et al., 2013).

Nevertheless, the literature is also indicating that there are growing difficulties related to privacy-oriented cryptocurrencies, decentralized finance services, cross-chain transfers of assets, and sophisticated methods of obfuscation. The developments heavily decrease the traceability of transactions and make it hard to conduct forensic attribution (Campisi and Celeste, 2021). Consequently, more flexible and scalable forensic approaches based on harmonized regulation and cross-border collaboration became the focus of recent research.

### 3.4 Gaps and Motivation in Research.

Regardless of significant advances in the dark web analysis, machine learning-related forensic tools, and blockchain-based analytics, current studies are disjointed across disciplinary lines. Bibliometric research offers a useful picture of research trends but is typically not all that technical, and algorithm research will typically test the performance of the model, not sufficiently considering legal, ethical and governance issues.

Furthermore, it is not yet entirely embraced to incorporate dark web intelligence, blockchain forensic analysis, and artificial intelligence into integrated systems of investigation. Majority of research deals with these areas independently and therefore there is no comprehensive research which discloses real world investigative processes. The current literature also lacks focus on ethical aspects, sustainability issues, and long-term governance systems.

Inspired by these gaps, this review aims to bring together research in the field of dark web studies and blockchain forensics alongside AI-based methods of investigations. The paper has tried to offer a varied viewpoint on capabilities currently available, contemporary issues, and future research directions that can facilitate secure, transparent, and ethically sound digital forensic investigations.

## 4.Techniques for Blockchain Forensics

Blockchain forensics is a conceptual framework of analyzing blockchain ledger data systematically to interpret, trace, and assign unlawful cryptocurrency dealings. Even though Blockchain systems are based on Pseudonymous identifiers, the public ledgers make transparency and immutability offer a useful source of forensic evidence to investigators.

### 4.1 Transaction Graph Analysis

A blockchain forensic tool is the fundamental technology in transaction graph analysis, which represents blockchain data as directed graphs. These graphs have nodes (wallet address or transaction), and the edges (flow of cryptocurrency). Investigators may follow the illicit money flow through many hops by studying the transaction paths, fund flows, and structural properties of these graphs to identify money laundering by chains, aggregation, and layering (Meiklejohn et al., 2013).

Graph-based measures, such as degree centrality, betweenness centrality, clustering coefficients, and shortest path lengths are used as tools to determine anomalous or high-risk actors to transaction networks. The methods have been useful in monitoring ransomware payments, detection of dark web marketplace escrow wallets, and discovering cash-out points at cryptocurrency exchanges (Moser et al., 2013). Most blockchain forensic investigations therefore rely on transaction graph analysis as their source of analysis

**4.2 Entities Attribution and Wallet Identification.**

Entity attribution implies association of several blockchain addresses to a single controlling entity, e.g. an individual user, a dark web marketplace, a mixing service, or a ransomware group. This is because users often create new wallet addresses to improve on privacy, making heuristic-based methods useful in detecting address clusters that may belong to the same entity in a forensic investigation.

Such common heuristics as the common-input ownership heuristic (when multiple addresses in a transaction are used by a single entity) and change address detection (when a transaction changes new addresses) are presented (Reid and Harrigan, 2013). Further analysis of behavioural patterns, such as frequency of transactions, value distribution and interaction with familiar services, can be used to identify a wallet.

Dark web investigations heavily rely on wallet attribution, which can help the investigator identify blockchain activity as a service or actor. Attribution techniques can greatly augment the evidentiary strength when used together with off-chain intelligence, e.g., exchange records, or seized servers, or forum activity (Androulaki et al., 2013).

**4.3 Techniques of Deanonymization.**

One of the purposes of deanonymization methods is minimizing the anonymity of blockchain users by connecting on-chain transaction data to off-chain sources of information. One of them is network-level analysis, where the pattern of transaction broadcast can be correlated with IP addresses or network behavior and used to determine the identity of the user (Biryukov et al., 2014). Such analysis can still have investigative opportunities despite the complications presented by the use of Tor, as timing correlations and misconfigurations still can be used.

Another deanonymization technique that is significant is cross-platform analysis, in which blockchain addresses are matched with data retrieved on a dark web forum or social media platform or marketplace infrastructure seized. Timeseries behavior, frequency of transactions and relations with regulated cryptocurrency exchanges requiring Know Your Customer (KYC) procedures also help in associating pseudonymous addresses with real-world identities (Meiklejohn et al., 2013).

Nevertheless, privacy-enhancing methods, like CoinJoin, stealth addresses, ring signatures, and privacy-oriented cryptocurrencies, are increasingly opposed deanonymization methods. These processes can largely decrease the accuracy of attributions and are still a dynamic field of study (Kappos et al., 2018).

**4.4 Forensic Tools and Analytical platforms.**

A large variety of dedicated tools and platforms are created to assist in blockchain forensic investigations. The popular commercial applications of the law enforcement and regulatory agencies are Chainalysis, Elliptic, CipherTrace, and TRM Labs. Such tools allow such functionalities as transaction tracking, entity labelling, risk rating, data visualization, and automatic warning (Chainalysis, 2024; Elliptic, 2023; TRM Labs, 2024).

Besides commercial solutions, open-source tools and blockchain explorers can also help researchers to extract and analyze data on transactions to be used in academics. BlockSci and

GraphSense will enable large-scale blockchain analytics and reproducible research and provide more transparency than proprietary tools (Dasaklis et al., 2020).
Even though there are more accuracy and operational support with commercial tools, the closed-source cracks the possibilities of methodological transparency and independent validation. Such a trade-off between efficiency and transparency is one of the key factors to consider in scholarly research and a court of law alike.

### 4.5 Blockchain Forensics and Machine Learning/Artificial Intelligence.

The blockchain information is growing exponentially which has led to application of machine learning and artificial intelligence to improve scale and the depth of analysis. Supervised learning models are also utilized to categorize transactions and wallet addresses into illicit and legitimate depending on the characteristics of the transactions, frequency, and network position (Yadav and Singh, 2022).
Unsupervised methods of learning, such as clustering and outlier detection, have been shown to work on detecting hitherto unknown criminal behaviour without having labeled data sets. The more advanced model like deep learning and graph neural network allow up to now modeling of complex transaction relationships and enhances detection accuracy of large blockchain networks (Osterrieder et al., 2024).
Although effective, AI-based forensic tools have been questioned on the issues of explainability, complexity, and admissibility in court. Black-box models can be highly accurate with little transparency that can diminish confidence in forensic inferences and create difficulties in the courtroom. In turn, current studies attach importance to the creation of explainable and legally justifiable AI models in blockchain forensics.

### 4.6 Challenges and Limitations.

Despite the development of Blockchain Forensic methods, A number of challenges still remain. Privacy-focused cryptocurrencies, decentralized exchange, cross-chain transfer of assets, and complex obfuscation mechanisms significantly limit the traceability of transactions and make them difficult to attribute (Campisi and Celeste, 2021). Besides, access to vital off-chain information that will enable effective investigations may be curtailed by jurisdictional issues and regulatory disparities.
To overcome these difficulties, the methodological innovation will have to be constant, interdisciplinary cooperation will have to be provided, and legal and regulatory frameworks will have to be more harmonized. In the absence of such efforts, it is possible that blockchain forensics will be limited in its effectiveness in the case of dark web investigations.

## 5. Methodology

### 5.1 Research Design

This research takes the systematic literature review approach to discuss the available studies on the dark web inquiries, blockchain forensic study, and artificial intelligence-driven investigation techniques. Qualitative synthesis methodology is used to combine conceptual frameworks, analytical approaches, and investigative processes that are found in the literature.
A systematic literature review is especially appropriate to cross-disciplinary fields like digital forensics where the study cuts across cybersecurity, criminology, data science, and legal studies. The synthesis of the results of these fields is expected to yield a more comprehensive insight into what blockchain analytics is and how it can be used in detecting dark web marketplaces (Dasaklis et al., 2020).

### 5.2 Literature Selection

The search of the relevant literature was carried out in the well-known academic databases, such as Scopus, IEEE Xplore, SpringerLink, Elsevier ScienceDirect, SSRN, and Google Scholar. The literature review is mainly related to the 2012-2025 era, which is associated with the dynamism of the dark web ecosystem, the blockchain, and the forensic approach.

The search strategy was based on structuring a combination of key words and Boolean operators such as:

- Dark web investigation
- Blockchain forensics
- Cryptocurrency tracing
- Transaction graph analysis

When applied to cyber forensics, machine learning is referred to as machine learning in cyber forensics.

Peer-reviewed journal articles, conference papers, and authoritative reports were only included to make sure that they are academic and relevant.

### 5.3 Inclusion Criteria and Exclusion Criteria

The inclusion criteria included the studies that examined the dark web activity, crimes linked to blockchain development, or digital forensic strategies to respond to cryptocurrencies analysis. Studies that were devoted to forensic systems, attribution methods, and ethical or legal aspects of investigations of cybercrime were also mentioned.

The exclusion criteria were based on the exclusion of non-academic sources, including blogs and opinion articles, and research with inadequate methodology or forensic significance. Articles that dealt with economics of cryptocurrency that include no investigative or forensic implications were also omitted.

### 5.4 Analysis of Data and Extraction

The chosen articles were systematically reviewed to obtain the data about the purpose of the research, the employed techniques of forensics (e.g., clustering, heuristic analysis, machine learning), analytical tools and platforms, empirically verified results, and the challenges reported. Thematic analysis method was used to sort out the findings into broad themes which included dark web ecosystems, blockchain forensic tools, artificial intelligence applications, case studies and future research directions.

### 5.5 Ethical and Considerations of validity.

Since the research on the dark web and cryptocurrency is rather sensitive, ethical considerations were thus taken into consideration. The review itself is based purely on secondary data sources and does not presuppose direct contact with the dark web resources or the personal information. This will reduce the risk of ethics and ensure validity and reliability of findings (UNODC, 2022).

## 6. Dark Web Investigation Case Studies.

Case studies of real-life investigation will offer a vital understanding of how blockchain analytics and digital forensic tools can be applied to dark web situations. The below-cases explain how blockchain forensics has played a vital role in tracing and breaking down significant criminal activities.

**6.1 The initially investigated case is that of Silk Road Marketplace.**
Silk Road market place is one of the pioneer and most impactful dark web researches. As an online loot of illegal drug deals, Silk Road depended mostly on Bitcoin. The blockchain transaction analysis developed by investigators helped trace the flow of Bitcoin out of the marketplace wallets to centralized exchanges. Law enforcement agencies were able to connect online activity with the corresponding real-world identities by matching patterns of transactions with operational security breaches such as reused usernames and misconfigured servers (Christin, 2013; Meiklejohn et al., 2013).
This case has shown that blockchain forensics can be used in the investigation of dark web crime, and that technology analysis should be combined with conventional investigative techniques.

**6.2 AlphaBay and Hansa Market Takedown.**
International cooperation and proactive investigation techniques proved to be effective as shown by the coordinated shutdown of AlphaBay and Hansa marketplaces. In its operation, the police took control of the Hansa marketplace secretly and kept operating it over a number of weeks. This method was able to gather user credentials, record of transactions, and communication logs.
Forensic analysis of blockchains was significant in tracking cryptocurrency payments, as well as connecting vendors and buyers to criminal operations. The operation revealed that evidence collection and attribution can be greatly improved with the help of managed platform management and blockchain analytics (Europol, 2023).

**6.3 Ransomware and Cryptocurrency Tracing: Colonial Pipeline Attack.**
The Colonial Pipeline ransomware episode highlighted how blockchain forensics can be extremely important when it comes to high-impact cybercrime investigations. Investigators tracked the money trail with the help of transaction graph analysis and wallet clustering methods after the ransom had to be paid in cryptocurrency. Part of the ransom was made back after determining that there was a wallet controlled by the attackers (Chainalysis, 2024).
This instance had shown that even highly advanced ransomware units that use cryptocurrency payments can still be tracked by forensics in some circumstances.

**6.4 Dark Web Financial Laundering Networks.**
Various studies have focused on dark web-based money laundering services, such as cryptocurrency mixing and tumbling services that are aimed at hiding the source of transactions. Investigators could identify service operators and wallet groups based on analyzing timing patterns and value distribution and interacting with known illicit wallets (Campisi & Celeste, 2021).
These ones showed the inherent flaws in the anonymization services and emphasized the role of heuristic-based and AI-assisted transaction analysis in identifying laundering schemes.

**6.5 Illicit Service Networks and Human Trafficking.**
The use of blockchain forensic methods has also been used in human trafficking and other networks of illicit services that run on the dark web. Under these circumstances, cryptocurrency payment trails are examined along with linguistic analysis, image metadata analysis, and undercover digital activity. Combining the blockchain analytics with content and behavioural forensic tools has already become crucial in aiding to support attribution and prosecution (UNODC, 2022).

## 7. Challenges and Limitations

**7.1 Privacy Enhancing Technologies and Reduced Traceability.**
Although blockchain forensics has progressed, the growing use of privacy-enhancing technologies is posing significant challenges to the traceability of the transactions. Cryptocurrencies, including Monero and Zcash, are privacy-orientated cryptocurrencies that use cryptographic constructions such as ring signatures, stealth addresses, and zero-knowledge proofs that obstruct transaction flows and attribution processes (Kappos et al., 2018). Also, coin mixing and tumbling provide extra services to undermine the transparency of transactions through the existence of deterministic connections between input and output addresses (Campisi and Celeste, 2021).

**7.2 Data Availability and Dataset Quality.**
The major weakness of blockchain forensic studies is the absence of publicly accessible real-world data involving activities in the dark web. Legal, ethical and operational limitations of access to genuine investigative information limit the use to artificial or slightly labeled datasets. Though they enable the methodological experimentation, they restrict the possibilities of generalization and a real-world applicability of suggested forensic models (Europol, 2023).

**7.3 Scalability and Computational Complexity.**
Blockchain networks are rapidly increasing in size and transaction count and the computer computation of the transaction graphs of large scale is computationally expensive. The problem of scalability is also exacerbated by cross-chain asset transfers and decentralized finance platforms, which divides the trail of transactions in more than one blockchain ecosystem. These issues will need to be tackled by using optimized algorithms, performance computing, and interoperable forensic frameworks (Osterrieder et al., 2024).

**7.4 Legal, Ethical and Privacy issues.**
Principles of legal and ethical concern the use of blockchain analytics and AI-based surveillance tools. The problems associated with the violation of privacy rights, the reasonableness of forensic models, and the fact that digital evidence can be explained, and its admissibility should be paid attention to. The discrepancies in the laws and regulatory structures of data protection in various jurisdictions complicate even more the cross-border investigation (UNODC, 2022).

**7.5 Nonsensitivity and International Co-ordination.**
Lack of unified forensics methodology and benchmarking systems restrains comparability and reproducibility of blockchain forensic research. Moreover, the crimes conducted with the help of the dark web are explicit to be transnational in nature, but the mechanisms of coordination and information exchange between countries are still inconsistent. The importance of better enforcement is in increased cooperation across the world and standardized standards in investigations (Europol, 2023).

## 8. Interaction with Classic Digital Forensics.

The field of blockchain forensics is most valuable when used along with the established computer forensic tools, such as computer forensics, network forensics, and log analysis. Although blockchain analytics allow to pursue the illegal movement of cryptocurrencies, the standard methods of work with forensics allow to refer wallets addresses to physical signs,

user accounts, and communication traces.
Research suggests that supporting blockchain-based intelligence with evidence collected in the compromised devices, server logs and exchange records contribute significantly to the attribution and the admissibility of the evidence (Meiklejohn et al., 2013). In addition, access patterns to anonymization networks like Tor can also be conveyed through network traffic analysis and traffic fingerprinting, which can also give further contextual support.
Heterogeneous forensic data sources are correlated through integration of machine learning techniques, which help an investigator to identify a behavioural pattern and determine more significant associations between on-chain and off-chain evidence. Nonetheless, effective integration must be accompanied by standardized data formats, interoperability of tools together with cross-domain knowledge among investigators.

## 9. New Trends and Future Direction.

### 9.1 Artificial Intelligent and Advanced Machine Learning.

Recent studies reveal that there has been a transition to the rule-based forensic approach to the data-driven AI methods that are able to process large volumes of blockchain and dark web information. This is evidenced by further models, like deep learning networks and graph neural networks that demonstrate progress in the recognition of transaction patterns, detection of anomalies, and profiling of behavior (Osterrieder et al., 2024).

### 9.2 Cross-Chain and Multi-Blockchain Forensic Analysis.

Due to the increasing popularity of the use of decentralized finance platforms and blockchain bridges as well as token swaps, it was required to use forensic tools that would be able to trace assets in heterogeneous blockchain ecosystems. The next area of study would be the cross-chain interoperability and standardized tracing mechanisms that would not lose the context of the transaction (Dasaklis et al., 2020).

### 9.3 Forensic Techniques to protect privacy.

The issue of the integrity of investigations between personal privacy rights is a major challenge. New strategies like selective disclosure, differentiated privacy, and privacy-preserving analytics are set to make it possible to perform verification of forensics with a minimum of the exposure of any data. Such methods can be used to overcome ethical and regulatory issues and not lose the confidence of the population (UNODC, 2022).

### 9.4 The Multimodal Dark Web Intelligence.

The combination of blockchain analytics, natural language processing, and social network analysis is becoming popular. Multimodal intelligence systems have the potential to augment situational awareness related to the dark web operations and facilitate the initial identification of the illicit activities (Yadav and Singh, 2022).

### 9.5 Standardization and International Co-operation.

The literature notes that there is a need to have harmonized forensic standards and enhancement of cooperation by international cooperation. It is crucial to create unified investigative models, intelligence libraries, and unified enforcement policies to deal with the transnational part of the dark web crime (Europol, 2023).

## 10. Research Gaps

This review notes that some of the research gaps are that there are no empirical benchmark datasets that researchers can use to verify their research, few forensic capabilities of privacy-centric cryptocurrencies, lack of cross-chain tracing systems, scalability and explainability of AI models, and lack of standardized ethical and legal regulations. The gaps should be filled to enhance effectiveness and sustainability of blockchain forensics in dark web investigations.

## 11. Conclusion

This review considered the changing application of blockchain analytics in detecting and exploring dark web markets. The evidence reveals that blockchain forensic tools like the analysis of transaction graphs, attributing entities, and Wallet identification are crucial in tracking illegal money flows of cryptocurrencies and assisting law enforcers. Scalability and detection have also been increased with the introduction of machine learning and artificial intelligence.

Nevertheless, there are still difficulties concerning privacy-enhancing technologies, the availability of data, the expansions of scales, and legal limitations. The solutions to these issues are interdisciplinary work, constant innovations in methodology, and unified regulatory systems. Finally, blockchain forensics and the conventional digital forensic practices and ethical governance framework must be integrated to achieve strong investigative powers that are able to deal with the increased complexity of dark web-supported cybercrime.

## References


1. Al-Nemrat, A., Jahankhani, H., & Preston, D. (2020). Cybercrime and the dark web: A systematic review. *International Journal of Cyber Security and Digital Forensics, 9*(1), 1–15.
2. Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in Bitcoin. In *Financial Cryptography and Data Security* (pp. 34–51). Springer.
3. Campisi, P., & Celeste, C. (2021). Cryptocurrency mixing services: Analysis and detection. *IEEE Transactions on Information Forensics and Security, 16*, 2089–2102.
4. Chainalysis. (2024). *Crypto crime report*. Chainalysis Inc.
5. Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd International World Wide Web Conference* (pp. 213–224).
6. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546.
7. Dasaklis, P., Casino, F., & Patsakis, C. (2020). Blockchain-based digital forensic tools: A classification and research outlook. In *IEEE Security and Privacy Workshops*.
8. Elliptic. (2023). *Cryptocurrency crime and blockchain analytics*. Elliptic Research Report.
9. Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA)*. Europol.
10. Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies, 32*(5),

1798–1853.

**11.** Gjorgjev, J., Ramadhan, M. F. F., & Dhamayana, S. (2025). Blockchain forensics: Unmasking anonymity in dark web transactions. *International Journal of Criminology and Sociology, 14*, 68–75.
**12.** Kappos, G., Yousaf, H., Maller, M., & Meiklejohn, S. (2018). An empirical analysis of anonymity in Zcash. In *Proceedings of the USENIX Security Symposium*.
**13.** Meiklejohn, S., Pomarole, M., Jordan, G., et al. (2013). A fistful of bitcoins: Characterizing payments among men with no names. In *Proceedings of the ACM Internet Measurement Conference*.
**14.** Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In *APWG eCrime Researchers Summit*.
**15.** Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.
**16.** Osterrieder, J., Lokhov, S., & Shams, T. (2024). Detecting anomalies and frauds in blockchain networks. *arXiv preprint arXiv:2402.11231*.
**17.** TRM Labs. (2024). *Illicit activity in the crypto ecosystem*. TRM Labs Intelligence Report.
**18.** UNODC. (2022). *Darknet cybercrime and cryptocurrencies*. United Nations Office on Drugs and Crime.
**19.** Yadav, S., & Singh, A. (2022). Machine learning techniques for cybercrime detection on the dark web. *Journal of Cybersecurity and Information Management, 6*(2), 45–58.

**20.** Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
**21.** Ron, D., & Shamir, A. (2013). Quantitative analysis of the full Bitcoin transaction graph. In *Financial Cryptography and Data Security* (pp. 6–24). Springer.
**22.** Spagnuolo, M., Maggi, F., & Zanero, S. (2014). BitIodine: Extracting intelligence from the Bitcoin network. In *International Conference on Financial Cryptography and Data Security*.
**23.** Soska, K., & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In *24th USENIX Security Symposium* (pp. 33–48).
**24.** Van Buskirk, J., Naicker, S., Bruno, R., Burns, L., & Breen, C. (2016). Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs. *International Journal of Drug Policy, 35*, 102–110.
**25.** Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2016). Going international? Risk taking by cryptomarket drug vendors. *International Journal of Drug Policy, 35*, 69–76.
**26.** Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213–238.
**27.** Chainalysis. (2023). *The geography of cryptocurrency*. Chainalysis Research.
**28.** FATF. (2021). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers*. Financial Action Task Force.

**29.** Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2018). When the cookie meets the blockchain. *Proceedings of the ACM CCS*.
**30.** Weber, M., Domeniconi, G., Chen, J., et al. (2019). Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks. *KDD Workshop on Deep Learning on Graphs*.

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.