**Detecting ‘&’ Mitigating Dark-Web Marketplaces**

**Yuvraj Singh Rawal,** [Shikha Agarwal](mailto:agarwalshikha@akgec.ac.in)**, Aarti Chaudhary**

Department of Information Technology

Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh, India

[yuvrajsinghrawal004@gmail.com](mailto:yuvrajsinghrawal004@gmail.com) s[hikhaagl03@gmail.com](mailto:shikhaagl03@gmail.com), [chaudhary.aarti111@gmail.com](mailto:chaudhary.aarti111@gmail.com)

**ABSTRACT**

Technologies such as TOR and I2P provide access to a section of the internet known as the dark web, which serves as a platform for countless illegal activities including drug dealing, arms trade, and counterfeiting. This study offers insight into the problem of identifying and combating dark web markets, particularly in regard to anonymity given encryption, non-centralized systems and the use of currencies such as Bitcoin. Already existing detection methods such as web scraping, machine learning content-based detection and blockchain surveillance are addressed as well as other measures such as law enforcement operations and provision of financial sanctions. An integrated tool is proposed which makes use of these technologies in order to improve detection in a real time manner - detection of dark web activities. Simultaneously, the ongoing development of AI and analysis of privacy coins paints a hopeful picture for more effective solutions against the dark web in the future.

**Keywords:** Dark Web Marketplaces, Anonymity and Encryption, Web Scraping and Machine Learning, Cryptocurrency Tracking, Blockchain Analysis

**1. INTRODUCTION**

The dark web, a concealed section of the internet accessible exclusively through specialized technologies such as The Onion Router (TOR) and the Invisible Internet Project (I2P), has emerged as a hub for illicit activities. The inherent anonymity and encryption provided by these networks enable individuals to evade detection and establish dark web marketplaces, where illegal goods and services—ranging from narcotics, firearms, and counterfeit currency to stolen data, illegal hacking services, and human trafficking—are traded with relative impunity. These clandestine platforms operate beyond the reach of traditional search engines and are fortified by decentralized systems, posing significant challenges for law enforcement agencies worldwide in tracking, monitoring, and dismantling such operations.

This research aims to comprehensively explore the complex landscape of detecting and mitigating dark web marketplaces, shedding light on the technical, operational, and legal structures that sustain these platforms. By examining the technological infrastructures—such as peer-to-peer networks, cryptographic techniques, and decentralized

hosting—that shield these marketplaces from visibility, the study reveals how they continue to flourish despite ongoing regulatory and enforcement efforts. Furthermore, it reviews a variety of emerging tools and methodologies being developed to counter illegal activities on the dark web. Among these are web scraping techniques used to systematically extract data from hidden marketplaces, machine learning algorithms that classify illegal content, and blockchain analysis methods that track cryptocurrency transactions commonly used to finance these illicit activities.

Central to the study is a critical evaluation of the current detection strategies employed by cybersecurity professionals and law enforcement. Key approaches discussed include the use of advanced machine learning models to identify patterns indicative of illegal trade, the development of algorithms to trace cryptocurrency flows and map transactional networks, and web scraping technologies designed to penetrate the layers of anonymity on dark web platforms. The research also highlights the need for an integrated, real-time tool that combines these technologies to improve the detection and mitigation of dark web marketplaces more effectively.

Finally, the study examines the legal and regulatory frameworks that could bolster the fight against dark web crime, proposing new approaches for cross-border collaboration, enhanced surveillance, and the potential for future advancements in artificial intelligence and blockchain analytics to create more resilient and effective strategies. This research emphasizes the urgency of a coordinated global effort to address the growing threat posed by dark web marketplaces, while also exploring forward-looking solutions that could shape the future of cybersecurity and digital law enforcement.

2.**Challenges in Detecting Dark-Web Marketplaces**

[Detecting dark web marketplaces is a tough challenge because of the advanced technologies that hide users' identities and activities. Here are some of the main hurdles when it comes to tracking down illegal marketplaces on the dark web:](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10695971/)

**[2.1 Anonymity through Encryption Technologies](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10695971/)**

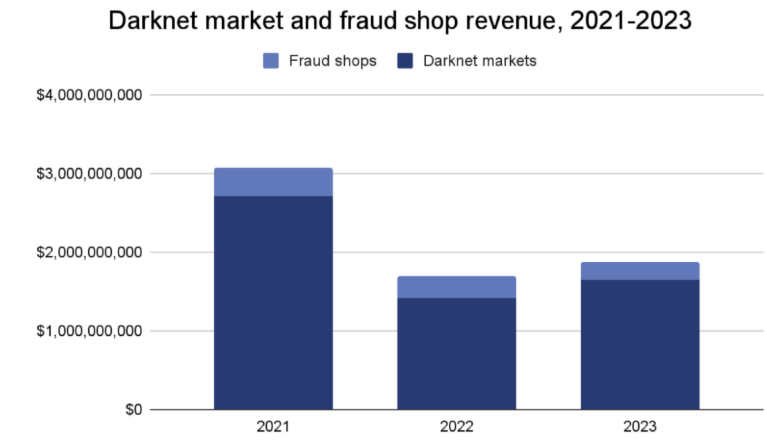
[The TOR network and other encrypted communication tools, like I2P, give users almost complete anonymity. For example, TOR works by routing traffic through several layers of encryption across multiple nodes, making it very difficult to trace a user’s original IP address. Most dark web marketplaces are hosted on “.onion” sites, which can’t be accessed by regular browsers or search engines. This anonymous and decentralized structure offers a safe haven for illegal activities, and law enforcement is often limited to monitoring only the external parts of the network, which doesn’t provide enough information to identify the people involved.](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10695971/)

**[2.2 The Decentralized Nature of Dark Web Marketplaces](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10695971/)**

[Dark web marketplaces are highly decentralized and constantly changing. When one marketplace is shut down, many new ones often pop up to take its place, making it feel like a never-ending game of Whack-a-Mole. After the shutdown of Silk Road, for example, replacements like AlphaBay and Dream Market quickly emerged. Even when these were taken down, others filled the gap. Users often switch between multiple marketplaces at once, which makes illegal operations even more scattered. In this fluid environment, law enforcement faces the massive challenge of trying to contain an ecosystem that keeps shifting and adapting.](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10695971/)

**2.3 Cryptocurrencies and Financial Anonymity**

Most dark web transactions use cryptocurrencies like Bitcoin, Monero, and Ethereum. While Bitcoin’s blockchain is publicly available and transparent, the identities of the users remain pseudonymous. To make things even more difficult, privacy tools like cryptocurrency mixers (or tumblers) are used to hide transaction histories, making it harder to trace funds. Cryptocurrencies offer a convenient way to launder money and carry out large-scale transactions without leaving the paper trails that traditional banking systems do.

[](https://www.chainalysis.com/blog/darknet-revenue-2023/)

Graph:1

**2.4 Ephemeral Marketplace Existence**

[Dark web marketplaces often have a short life span, closing abruptly either because of law enforcement interventions or](https://www.emcdda.europa.eu/system/files/publications/2155/TD0416925ENN.pdf)

[voluntary exits by marketplace operators. This transient nature makes it extremely difficult to maintain a reliable index of illegal marketplaces. Constantly changing URLs, encrypted communications, and quick migrations mean that traditional web crawling techniques are insufficient to monitor this evolving environment. Law enforcement and cybersecurity agencies require continuous updates to their intelligence-gathering techniques in order to track the ever-shifting terrain of the dark web.](https://www.emcdda.europa.eu/system/files/publications/2155/TD0416925ENN.pdf)

**[3. Existing Detection Techniques for Dark Web Marketplaces](https://www.emcdda.europa.eu/system/files/publications/2155/TD0416925ENN.pdf)**

[Despite the challenges, there’s been considerable progress in detecting and tracking dark web marketplaces. Various tools and techniques have been developed to monitor these activities, and here are some key methods:](https://www.emcdda.europa.eu/system/files/publications/2155/TD0416925ENN.pdf)

**[3.1 Web Crawling and Data Collection](https://www.emcdda.europa.eu/system/files/publications/2155/TD0416925ENN.pdf)**

[Web crawling is at the core of detecting dark web marketplaces. Specially designed crawlers navigate hidden services like TOR, identifying active marketplaces, forums, and other sources of illegal activity. These crawlers gather product listings, user reviews, forum posts, and other data, creating a structured database for further analysis. However, since dark web marketplaces often shut down or move, these crawlers need constant updates to stay effective.](https://www.emcdda.europa.eu/system/files/publications/2155/TD0416925ENN.pdf)

[Smart crawlers use advanced algorithms to focus on high-value data, making sure they target the most relevant pages. They’re also built to uncover hidden URLs and get around barriers like CAPTCHAs or login screens, which often block access to dark web content.](https://www.emcdda.europa.eu/system/files/publications/2155/TD0416925ENN.pdf)

**3.2 Machine Learning for Content Classification**

Machine learning plays a crucial role in sorting through the content collected by web crawlers, helping to distinguish between legal and illegal activities. Some common models include:

**Support Vector Machines (SVMs):** These models classify text and images into categories like "legal" or "illegal." For example, SVMs can help detect listings for illegal drugs, stolen data, or firearms.

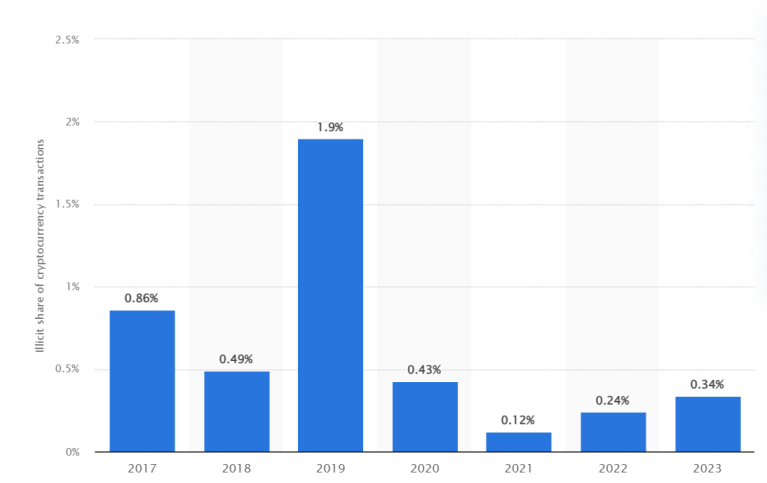
**Naïve Bayes Classifiers:** Using a probabilistic approach, this model can classify content based on the likelihood that certain words or phrases point to illegal activities. It’s particularly useful for analyzing forum discussions and user-generated content.

**Random Forests and Decision Trees:** These models are great for structured data like product listings and transactions. They can spot illegal activity by looking at variables like product descriptions, price ranges, or seller reputations.

Machine learning models are continuously trained on new data, improving their accuracy over time. With enough data, they can reach impressive precision, often identifying illegal activities with more than 90% accuracy.

**3.3 Blockchain Analysis for Cryptocurrency Tracking**

[Blockchain analysis is essential for tracking cryptocurrency transactions on dark web marketplaces. While blockchain itself is a public ledger where all transactions are recorded, the identities of the users are pseudonymous. Companies like Chainalysis and Elliptic have developed tools to trace cryptocurrency transactions, helping to pinpoint clusters of illegal activity. By following the flow of cryptocurrency, investigators can link transactions to specific wallets or individuals involved in dark web activities.](https://www.chainalysis.com/blog/darknet-revenue-2023/)

[](https://www.chainalysis.com/blog/darknet-revenue-2023/)Graph:2

[Transaction Mapping: By mapping the flow of transactions, blockchain analysis can identify connections between dark web users. Law enforcement can analyze large transaction patterns to identify wallet addresses used for illegal transactions, even tracing the movement of funds through mixers or exchanges.](https://doi.org/10.1038/s41598-023-50409-5)

[Wallet Clustering: Blockchain analytics can also cluster wallet addresses associated with a single user or entity. These clusters are used to trace the broader financial network of illegal actors on the dark web.](https://doi.org/10.1038/s41598-023-50409-5)

[Despite the success of blockchain analysis, challenges remain, particularly when users employ privacy-focused cryptocurrencies like Monero, which are designed to obscure transaction details entirely.](https://doi.org/10.1038/s41598-023-50409-5)

**Social Network and Transactional Network Mapping**

[Analyzing social and transactional networks on the dark web helps identify key players and their interactions. Law enforcement agencies use network mapping tools to create visual representations of connections between buyers, sellers, and intermediaries. These maps allow investigators to pinpoint influential users—such as high-volume sellers or intermediaries operating across multiple marketplaces—and prioritize their investigation.](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10695971/)

[Network analysis also uncovers the resilience of the marketplace ecosystem, demonstrating how users and marketplaces are interconnected. Understanding these connections helps agencies target key individuals to have a more significant impact on the dark web ecosystem.](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10695971/)

**4. Mitigation Strategies for Dark Web Marketplaces**

[Once illegal activities on the dark web are identified, there are several strategies that can be used to disrupt these marketplaces. These strategies range from taking down the marketplaces directly to cutting off their financial lifelines.](https://www.researchgate.net/publication/361242066_Dark_Web_Illegal_Activities_Crawling_and_Classifying_Using_Data_Mining_Techniques)

**[4.1 Coordinated Law Enforcement Takedowns](https://www.researchgate.net/publication/361242066_Dark_Web_Illegal_Activities_Crawling_and_Classifying_Using_Data_Mining_Techniques)**

[One of the most publicized ways to disrupt dark web marketplaces is through law enforcement takedowns. High-profile operations like the shutdowns of Silk Road, AlphaBay, and Hansa have shown how authorities can dismantle major dark web platforms. These efforts usually involve seizing the marketplace’s servers, arresting its operators, and confiscating any cryptocurrency used in the illegal trades.](https://www.researchgate.net/publication/361242066_Dark_Web_Illegal_Activities_Crawling_and_Classifying_Using_Data_Mining_Techniques)

[However, takedowns aren’t a permanent fix. History has shown that when one marketplace goes down, others quickly emerge to take its place. That’s why law enforcement agencies are increasingly working together globally, targeting multiple platforms at once to have a longer-lasting effect.](https://www.researchgate.net/publication/361242066_Dark_Web_Illegal_Activities_Crawling_and_Classifying_Using_Data_Mining_Techniques)

**[4.2 Financial Disruption through Blockchain Analysis](https://www.researchgate.net/publication/361242066_Dark_Web_Illegal_Activities_Crawling_and_Classifying_Using_Data_Mining_Techniques)**

[Disrupting the flow of money is another powerful way to cripple dark web operations. By collaborating with blockchain analysis firms, law enforcement can track cryptocurrency transactions to specific wallets used in illegal activities. Once these wallets are identified, cryptocurrency exchanges and financial institutions can freeze the assets or flag them for further investigation, making it harder for criminals to conduct business on the dark web.](https://www.researchgate.net/publication/361242066_Dark_Web_Illegal_Activities_Crawling_and_Classifying_Using_Data_Mining_Techniques)

[Additionally, there are efforts to improve regulations, such as stronger Know Your Customer (KYC) and Anti-Money Laundering (AML) processes at cryptocurrency exchanges. These measures make it more difficult for dark web users to convert their illicit funds into cash anonymously.](https://www.researchgate.net/publication/361242066_Dark_Web_Illegal_Activities_Crawling_and_Classifying_Using_Data_Mining_Techniques)

**4.3 Monitoring and Infiltrating Dark Web Forums**

Dark web forums are the places where buyers and sellers communicate, exchange tips on avoiding detection, and recruit new members. By monitoring these forums, law enforcement can gather valuable intelligence about emerging threats, new marketplaces, and key players.

Cybersecurity experts and law enforcement use techniques like web scraping and Natural Language Processing (NLP) models to sift through massive amounts of text and identify conversations related to illegal activities. In some cases, undercover agents even join these forums to build relationships with key figures and gather critical intelligence that can lead to further action.

**5. Proposed Real-Time Detection and Mitigation Tool**

This research introduces an advanced, integrated tool designed to detect and mitigate illegal activities on dark web marketplaces. It leverages machine learning, blockchain analysis, web crawling, network mapping, and real-time alerts to provide law enforcement agencies with a comprehensive solution for tracking and disrupting dark web activities.

**5.1 Web Crawler and Scraper Module**  
The web crawler and scraper form the core of the tool, designed to navigate hidden services on the dark web (such as TOR and I2P networks). The module is optimized for gathering data from marketplaces, forums, and other dark web resources, even in environments with obfuscation techniques like CAPTCHAs or login barriers.

**Key Features**:

**TOR Network Integration**: Utilizes a specialized crawler that operates within the TOR network, maintaining complete anonymity using Python libraries like Stem.

**Dynamic Crawling**: Continuously updates its database, adapting to the transient nature of marketplaces by detecting new URLs as they migrate or go offline.

**CAPTCHA Solving**: Employs automated CAPTCHA-solving techniques or third-party APIs to bypass login and security measures.

**Data Collection**: Extracts structured data, including product listings, user profiles, and transaction logs from dark web marketplaces for analysis.

**Technologies**:

Python web scraping libraries (Scrapy, BeautifulSoup)

TOR library (Stem) for .onion site access

CAPTCHA bypass tools (AntiCaptcha, 2Captcha)

**5.2 Machine Learning Classifier for Content Identification**  
This module processes data gathered by the web crawler, using machine learning to distinguish between legitimate and illegal activities by analyzing both text and images.

**Key Features**:

**Text Classification**: Trains models using Support Vector Machines (SVMs) or Natural Language Processing (NLP) techniques to detect keywords and phrases associated with illegal items (drugs, firearms, hacking tools).

**Image Classification**: Utilizes image recognition technology to analyze visual content from listings and identify illegal items such as weapons or contraband.

**Continuous Training**: Ensures classifiers are continuously updated to adapt to evolving language and techniques used on the dark web.

**Technologies**:

Machine learning libraries (TensorFlow, scikit-learn)

NLP tools (spaCy, NLTK)

Image recognition models (OpenCV, Keras)

**5.3 Blockchain and Transaction Analysis Engine**  
Since cryptocurrency is the primary medium of exchange on dark web marketplaces, this module tracks cryptocurrency transactions to detect illegal activities.

**Key Features**:

**Transaction Tracking**: Analyzes blockchain transactions to identify suspicious patterns and link them to dark web activities using APIs from services like Chainalysis and Elliptic.

**Wallet Clustering**: Groups wallet addresses linked to the same entity, allowing for tracking the flow of funds across multiple wallets and exchanges.

**Mixers and Tumblers Detection**: Identifies cryptocurrency laundering techniques such as mixers, which obscure the origin of funds.

**Real-Time Alerts**: Sends immediate alerts when suspicious transactions are detected, enabling fast law enforcement action.

**Technologies**:

Blockchain analysis APIs (Chainalysis, Elliptic)

Python blockchain libraries (Bit, PyMonero)

Transaction monitoring tools (GraphSense, CipherTrace)

**5.4 Network Mapping Engine**  
This engine visually maps the relationships between users, marketplaces, and financial transactions, helping investigators identify key actors and their influence within the dark web ecosystem.

**Key Features**:

**Social Network Analysis**: Maps interactions between buyers, sellers, and intermediaries to identify central figures in illegal operations.

**Transactional Network Mapping**: Visualizes the flow of cryptocurrency between wallets, identifying illegal clusters and connections across marketplaces.

**Graph Visualization**: Generates real-time graphical representations of marketplace networks, highlighting high-risk actors and their relationships.

**Technologies**:

Graph databases (Neo4j, GraphQL)

Python libraries for network mapping (NetworkX, PyGraphviz)

Visualization tools (Gephi, Cytoscape)

**5.5 User Interface and Dashboard**  
The tool includes a user-friendly dashboard that allows law enforcement or cybersecurity professionals to monitor, search, and analyze dark web activity in real time.

**Key Features**:

**Real-Time Monitoring**: Displays updates on new listings, marketplace statuses, and cryptocurrency flows.

**Search and Filtering Options**: Enables keyword-based searches for specific illicit items or marketplace names.

**Alert System**: Notifies users of new illegal activities or suspicious transactions.

**Detailed Reports**: Generates comprehensive reports on detected illegal activities, including data from web crawlers, classifiers, and blockchain analysis for use in investigations.

**Technologies**:

Frontend frameworks (React, Vue.js)

Backend frameworks (Node.js, Django)

Data visualization libraries (D3.js, Chart.js)

**5.6 AI-Powered Predictive Models**  
This module enhances proactive detection by predicting new dark web marketplaces and emerging illicit products based on historical trends and user behaviors.

**Key Features**:

**Marketplace Prediction**: Forecasts the emergence of new marketplaces after previous ones are shut down, based on user migration patterns.

**Emerging Threat Detection**: Detects the introduction of new illicit products or services by monitoring forums and private groups.

**Risk Scoring**: Assigns risk scores to marketplaces based on size, number of illegal listings, and transaction volumes, allowing law enforcement to focus efforts.

**Technologies**:

Deep learning frameworks (PyTorch, Keras)

Time-series analysis (Prophet, ARIMA)

By combining these advanced components, we can develop a comprehensive detection and mitigation tool that significantly enhances the ability to track and disrupt dark web marketplaces. The tool will provide law enforcement agencies with real-time insights and actionable data, allowing them to take down illegal operations with greater efficiency and precision.

**Future Approaches and Enhancements**

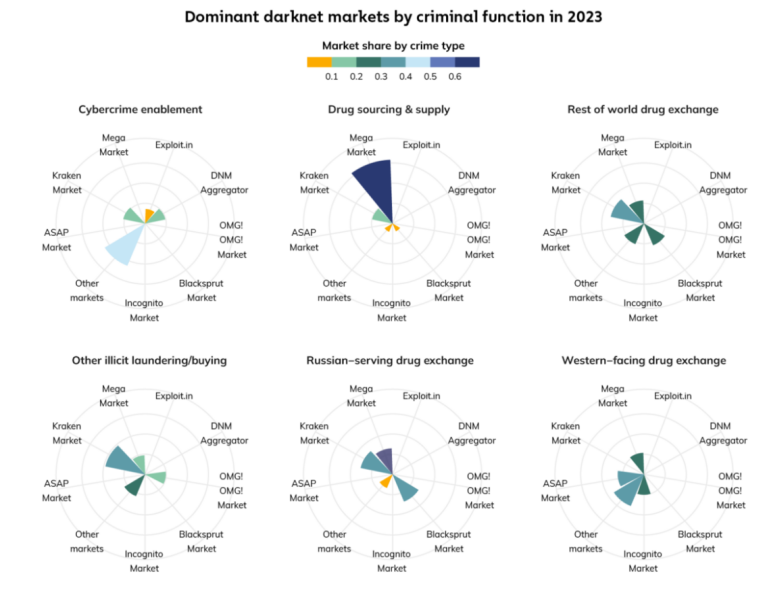
As dark web activities evolve, the tools and strategies used to combat them need to keep up. Here are some future approaches that could enhance how we detect and take down dark web marketplaces:

**6.1 AI-Powered Predictive Models**

A promising future approach involves using AI-powered models that can predict when and where new dark web marketplaces will appear. By analyzing patterns in past activity, these models can anticipate the rise of new markets before they fully take off. This would allow law enforcement to step in early, monitor potential threats, and shut them down before they gain momentum.

**6.2 Improved Privacy Coin Tracking**

While current tools are great at tracking transparent cryptocurrencies like Bitcoin, privacy-focused coins like Monero pose a bigger challenge. Future improvements in privacy coin analysis aim to tackle these hidden transactions. Techniques like Zero-Knowledge Proofs (ZKPs) could be used to spot illegal activities without compromising the privacy of legitimate users.

[](https://www.chainalysis.com/blog/darknet-revenue-2023/)

Graph:3

**6.3 Real-Time Takedown Strategies**

As dark web marketplaces become faster and more decentralized, being able to take them down in real-time will be key. The next generation of tools will enable law enforcement agencies to share information instantly and work together globally to shut down multiple marketplaces at once. Plus, when new marketplaces pop up in response to law enforcement actions, AI-powered detection tools will help neutralize them more quickly.

**6.4 Stronger Public-Private Collaboration**

The future of tackling dark web crime also relies on stronger teamwork between the public and private sectors. Cybersecurity companies, cryptocurrency exchanges, financial institutions, and government agencies need to join forces to create a unified approach to monitoring and stopping dark web activities. By sharing intelligence and updating cryptocurrency regulations, this collaboration can build a stronger system to detect and combat illegal activities.

**Conclusion**

Fighting against illegal activities on the dark web is an ongoing challenge that requires constant evolution and the use of cutting-edge technologies. As the dark web grows and adapts, so must the tools and strategies we use to combat its criminal activities. By using tools like machine learning, blockchain analysis, and network mapping, law enforcement and cybersecurity experts can better detect and disrupt the criminal networks operating in the hidden parts of the internet.

This research introduces a comprehensive tool designed to tackle the complex world of dark web marketplaces. By combining real-time web scraping, machine learning algorithms, blockchain tracking, and network mapping, this tool offers a powerful way to spot and disrupt illegal activities on the dark web. Looking ahead, advancements in AI, privacy coin analysis, and real-time takedown methods will make these efforts even more effective.

While the dark web remains a tough space to monitor and control, the development of smarter detection technologies offers hope. With continued innovation and collaboration between global teams, we can reduce the influence of illegal marketplaces and help create a safer online environment for everyone.

References

1. Fanusie, Y. J., & Robinson, T. (2023). *Identifying key players in dark web marketplaces through Bitcoin transaction networks.* Scientific Reports, 13, Article 50409. <https://doi.org/10.1038/s41598-023-50409-5>
2. Pramanik, S., Mondal, S., & Saha, S. (2022). *Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques.* ResearchGate.<https://www.researchgate.net/publication/361242066_Dark_Web_Illegal_Activities_Crawling_and_Classifying_Using_Data_Mining_Techniques>
3. Chainalysis. (2023). *Share of illicit transactions in all cryptocurrency transactions worldwide from 2017 to 2023.*<https://www.chainalysis.com/blog/darknet-revenue-2023/>
4. Alqahtani, A., Ghasemaghaei, M., & Hassani, H. (2023). *Darkweb research: Past, present, and future trends, and mapping to sustainable development goals.* Frontiers in Big Data, 6, Article 10695971.<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10695971/>
5. Chertoff, M., & Simon, L. (2021). *The Dark Web Phenomenon: A Review and Research Agenda.* ArXiv.<https://arxiv.org/pdf/2104.07138>
6. Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). *Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?* The Review of Financial Studies, 32(5), 1798-1853. https://doi.org/10.1093/rfs/hhz017
7. Soska, K., & Christin, N. (2015). *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem.* In Proceedings of the 24th USENIX Security Symposium (pp. 33-48). https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska.pdf
8. Xu, X., & Zheng, Z. (2020). *A Survey on Privacy and Security in Bitcoin: Toward Future Directions.* ACM Computing Surveys, 53(3), Article 63. https://doi.org/10.1145/3380998
9. Christin, N. (2013). *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace.* In Proceedings of the 22nd International Conference on World Wide Web (pp. 213-224). https://doi.org/10.1145/2488388.2488408
10. Kethineni, S., Cao, Y., & Dodge, C. (2018). *Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes.* American Journal of Criminal Justice, 43(2), 141-157. https://doi.org/10.1007/s12103-017-9394-6
11. Huang, D. Y., Xu, Z., & Whinston, A. B. (2018). *Directing traffic: Cryptocurrencies, darknet markets, and online crime.* Journal of Financial Economics, 130(3), 836-861. https://doi.org/10.1016/j.jfineco.2018.01.004
12. Aldridge, J., & Décary-Hétu, D. (2016). *Cryptomarkets and the future of illicit drug markets.* In EMCDDA (Eds.), *The internet and drug markets* (pp. 23-32). European Monitoring Centre for Drugs and Drug Addiction.<https://www.emcdda.europa.eu/system/files/publications/2155/TD0416925ENN.pdf>
13. Van Wegberg, R., Oerlemans, J. J., & van Deventer, O. (2018). *Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin.* Journal of Financial Crime, 25(2), 419-435. https://doi.org/10.1108/JFC-11-2016-0067
14. Möser, M., Böhme, R., & Breuker, D. (2013). *An inquiry into money laundering tools in the Bitcoin ecosystem.* In Proceedings of the APWG Ecrime Researchers Summit (pp. 1-14). https://doi.org/10.1109/ECRS.2013.6805780
15. Phetsouvanh, R., Ignatov, D. I., Batet, M., & Shekhovtsov, A. (2020). *Darknet markets ecosystem: Estimation and models.* Expert Systems with Applications, 144, 113072. https://doi.org/10.1016/j.eswa.2019.113072