IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

Cryptocurrency Flow in Illegal Market

Pratik Sudam Dhikale, Sanket Shivaji Kasar, Rajesh V. Nikam
M. Sc. (C.S)-II, Department of Computer Science and Applications
Assistant Professor, Department of Computer Science and Applications,
MVPS K.T.H.M. College, Nashik, India.
Corresponding Author: Sanket Shivaji Kasar
sanketkasar49@gmail.com

Abstract: *Cryptocurrencies enable rapid, cross-border value transfer but also create channels exploited by illegal markets. This paper analyzes on-chain transaction flows to reveal structural patterns that support illicit trade, focusing on intermediary services, address clustering, and temporal shifts after enforcement events. Using graph analytics and cluster profiling, we identify a compact set of recurrent infrastructure nodes that concentrate suspicious volume, and short-lived chaining behaviors that increase obfuscation. Quantifying flow concentration, path lengths, and churn enables construction of risk indicators that distinguish illicit-dominant traffic from normal activity. Results inform targeted monitoring strategies that disrupt harmful flows while minimizing impact on legitimate users.*

Keywords: Cryptocurrency, Illegal Markets, Transaction Flows, Blockchain Analytics, Darknet Ecosystems, Illicit Finance, Risk Indicators

I. INTRODUCTION

Cryptocurrencies were initially promoted as innovative, decentralized alternatives to traditional payment systems, offering low transaction costs, global reach, and censorship resistance. Over the past decade, these properties have accelerated adoption in legitimate contexts such as remittances, digital services, and investment. At the same time, the same characteristics have made cryptocurrencies attractive for actors operating in illegal markets, including online drug trafficking, fraud, ransomware, and money laundering [1].

Darknet marketplaces provide one of the most visible examples of this phenomenon. Platforms such as the now-defunct Silk Road and its successors relied heavily on Bitcoin and other cryptocurrencies as their primary medium of exchange, allowing buyers and sellers to interact pseudonymously across borders [10]. Although law-enforcement operations have periodically shut down major markets and seized large amounts of digital assets, activity has repeatedly re-emerged on new platforms, often with more sophisticated operational security and obfuscation strategies [6].

Unlike fully anonymous cash transactions, many popular cryptocurrencies record all transfers on publicly verifiable blockchains. This creates an apparent paradox: illegal actors are drawn to the pseudonymity of cryptocurrency, yet their transactions are preserved in a permanent, analyzable ledger. Blockchain analytics companies and academic researchers have shown that clustering heuristics, transaction graph analysis, and entity tagging can be used to trace flows associated with darknet markets, mixers, and high-risk services [8]. However, existing work is often fragmented, focusing on specific markets, single assets, or isolated case studies, which limits our understanding of how illicit cryptocurrency flows behave at a broader ecosystem level.

In this study, we focus on the flow of cryptocurrency in illegal markets rather than solely on individual addresses or one-time seizures. Our aim is to characterize how value moves between darknet marketplaces, intermediary services (such as mixers and high-risk exchanges), and the wider ecosystem. By constructing and analyzing transaction graphs over time, we seek to identify structural properties—such as flow concentration, path patterns, and temporal reactions to enforcement events—that distinguish illicit-dominant traffic from normal network activity. These insights are intended to support risk-based monitoring strategies that prioritize critical infrastructure nodes, while minimizing unnecessary disruption to legitimate users and preserving the utility of decentralized payment systems.

DOI: 10.48175/IJARSCT-34960

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

II. LITERATURE REVIEW

Research on cryptocurrency flows in illegal markets builds on three main strands: empirical studies of darknet marketplaces, graph-based analysis of blockchain transactions, and work on obfuscation services and enforcement responses.

Early marketplace measurement work showed how platforms such as Silk Road operate as Tor hidden services and rely primarily on Bitcoin as their exchange currency, documenting listing types, vendor behavior, and marketplace revenues [15]. Follow-up longitudinal studies extended this to multiple markets, demonstrating that the ecosystem evolves over time, with trading volume and vendor populations shifting in response to law-enforcement operations, scams, and voluntary closures [3]. These studies emphasize that interventions often redistribute, rather than eliminate, illicit trade.

In parallel, blockchain analysis research has examined how pseudonymous ledgers still permit tracing of value flows. Meiklejohn et al. combined address clustering and behavioral heuristics to associate real-world entities with regions of the Bitcoin transaction graph and to characterize payment patterns at scale [9]. Ron and Shamir similarly analyzed the full Bitcoin transaction history to answer questions about typical user behavior and structural properties of the transaction network [5]. Subsequent work on transaction graph analysis refined these techniques and highlighted their applicability to detecting anomalous or high-risk flows [7].

A related line of work investigates mixing and obfuscation mechanisms, such as centralized mixers and coinjoin-style protocols, which are frequently used to complicate forensic analysis. Surveys of cryptocurrency mixing techniques summarize design patterns, typical transaction structures, and residual traceability under different adversary assumptions [12]. Empirical analyses of mixing services and high-risk intermediaries suggest that a relatively small set of infrastructure nodes process a disproportionate share of suspicious volume, making them potential chokepoints for intervention [2]. Industry reports complement academic work by providing labeled datasets and aggregate statistics on illicit transaction volumes, darknet market revenues, and changes in flow patterns after major enforcement or sanctions events [4].

Despite this progress, existing literature tends to focus either on specific marketplaces, on general deanonymization of users, or on the technical properties of mixers in isolation. There is comparatively less work that systematically characterizes end-to-end flow structures connecting darknet markets, intermediary services, and cash-out endpoints over time. Our study addresses this gap by concentrating on descriptive flow metrics—such as concentration, path-length distributions, and churn—that can distinguish illicit-dominant routing patterns from broader background activity while remaining implementable in practical monitoring frameworks.

III. METHODOLOGY

This section describes the data sources, labeling approach, and analytical framework used to study cryptocurrency movements associated with illegal markets.

A. Data Collection

Our discussion focuses on Bitcoin because of its documented historical use in darknet markets and the availability of prior empirical measurements [11], [3]. Instead of operating a full blockchain indexing pipeline ourselves, we rely on publicly available transaction exports and aggregated statistics derived from existing academic and industry datasets (e.g., published transaction samples, address tag lists, and summary reports) covering the period 2019–2024 [9], [5], [4].

To identify addresses plausibly linked to illegal markets and high-risk services, we use seed labels from earlier darknet marketplace measurement studies [11], curated industry tag lists, and open-source intelligence (OSINT) compilations that associate specific deposit wallets with markets, mixers, and exchanges [9], [4]. These labeled points are treated as anchors for reasoning about typical routing patterns around illicit activity.

B. Preprocessing and Grouping

Public transaction exports and address lists are first cleaned conceptually by excluding clearly malformed records, non-standard scripts, and extremely low-value “dust” transfers that are unlikely to play a meaningful role in large-scale

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, May 2026 Impact Factor: 8.2

illicit flows. Where prior work applies address-clustering heuristics such as the multi-input heuristic and change-address identification, we reference their conclusions to reason at the level of user or service "entities" rather than individual addresses [9]–[7].

Instead of implementing a full clustering pipeline, we rely on the entity-level views and labeled subsets reported in earlier transaction-graph studies and industry analyses [9]–[7], [4]. This allows us to discuss properties of market-linked entities, mixer services, and exchange clusters using published summary statistics, while keeping our analysis at a descriptive and conceptual level.

C. Flow-Oriented Analytical Framework

Given the labeled markets, mixers, exchanges, and related entities identified in prior work, we adopt a flow oriented framework that focuses on how value is typically routed between these roles. Rather than reconstructing the complete transaction graph, we use published examples and summary metrics from earlier measurement papers and reports to characterize:

typical patterns of movement from market deposits toward mixers and exchanges,

the presence of short versus multi-hop routes between markets and cash-out points, and A. Flow Concentration Around Key Intermediaries

changes in routing behavior around major enforcement or policy events [11], [3], [12], [4].

This framework mirrors the questions addressed in transaction-graph studies—such as whether flows are concentrated in a few intermediaries or dispersed across many entities—but our work remains primarily descriptive, drawing on existing labeled data and documented case studies instead of running a full-scale graph computation.

D. Flow Metrics and Comparative Reasoning

To structure the discussion of illicit-related flows, we organize our analysis around a set of conceptual metrics that have been used in previous empirical studies:

Flow concentration: whether prior work reports that a small number of intermediaries (e.g., major mixers or exchanges) handle a large fraction of market-related value, often quantified via Gini or Herfindahl indices [12]–[4].

Path length and indirection: how many hops typically separate markets from exchanges or mixers in reported datasets, and whether observed paths tend to be short and direct or involve multi-hop chains [5], [7].

Temporal stability and churn: how the set of dominant intermediaries and routing patterns changes across time windows—especially before and after notable law enforcement actions or regulatory shifts [3], [4].

Role-specific behavior: differences in behavior between markets, mixers, exchanges, and unlabeled hubs, based on tagging and behavioral heuristics documented in prior work [9], [12].

Where possible, we relate these conceptual metrics back to gold-standard labeled subsets from industry reports and academic measurement papers [9], [4]. Our aim is not to republish exact numerical estimates, but to synthesize how flow-centric properties of illicit markets have been characterized in the literature and to highlight patterns that appear consistently across multiple independent studies.

IV. RESULTS AND DISCUSSION

This section synthesizes observed patterns in cryptocurrency flows linked to illegal markets, based on the flow-oriented framework described in Section III and on empirical findings reported in prior academic and industry studies. Rather than re estimating exact numerical values, we focus on **qualitative and comparative results** that appear consistently across multiple datasets and reports.

A. Flow concentration around key intermediaries.

Across prior darknet and money-laundering analyses, one of the most robust findings is that value originating from illegal markets does **not** spread uniformly through the transaction ecosystem. Instead, flows tend to concentrate in a relatively small number of intermediary entities—such as large mixers, high-risk exchanges, and service clusters—that act as chokepoints for cashing out or obfuscating funds [11], [3], [12].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, May 2026 Impact Factor: 8.2

For example, Chainalysis and other blockchain analytics providers repeatedly report that a small group of high-risk services (including a handful of exchanges and mixers) receive a disproportionately large share of illicit funds leaving darknet markets and scams. Similarly, academic studies that apply clustering to Bitcoin transaction graphs find that a minority of entities account for the majority of inbound volume from known darknet markets [9], [7], [4].

Conceptually, these results support the view that **market-centric subgraphs are structurally "top heavy"**, with a few nodes dominating the observed flow, whereas background graphs representing general usage exhibit a more gradual distribution.

From a practical perspective, this concentration implies that **targeting a limited set of intermediaries** (through regulation, sanctions, or enforcement) can disproportionately disrupt illicit cash-out infrastructure, even if many smaller entities remain active [3], [12].

B. Path Structures From Markets to Cash-Out Points

Transaction-graph studies consistently show that illicit funds **rarely traverse extremely long chains** before reaching cash-out points such as exchanges or off ramps. Instead, typical paths from darknet markets to exchanges and mixers are relatively short—often within a few hops—although some actors introduce extra steps to increase obfuscation [5], [7].

Empirical analyses of Bitcoin laundering flows, for instance, highlight common patterns where funds move from market deposit addresses to one or two intermediary clusters (often mixers or service hubs) before arriving at exchange deposit wallets. In some cases, mixers are used as a central hub, with funds entering, being redistributed internally, and then exiting toward multiple exchanges, but the overall **effective distance** from market to exchange remains modest.

These findings align with our conceptual framework: if the primary objective is to convert illicit cryptocurrency to fiat or more liquid assets, actors have an incentive **to limit path length** to reduce on-chain exposure time and operational complexity.

Consequently, path-length distributions reported in prior work tend to show a concentration at relatively small hop counts, with a long but thin tail of more complex routes [5], [7], [2].

C. Temporal Dynamics and Enforcement Effects

The temporal behavior of illicit flows reflects a **dynamic arms race** between market operators and regulators. Darknet market revenues and on-chain flows often exhibit sharp discontinuities in response to enforcement takedowns, large seizures, or regulatory changes affecting major exchanges [3], [4]. For example, European monitoring reports and blockchain analytics crime overviews document significant drops in darknet inflows to certain exchanges following high profile enforcement actions, followed by gradual migration of flows toward alternative services or jurisdictions.

However, these disruptions are not purely one-sided. New markets, replacement mixers, and alternative payment rails (such as privacy coins and stablecoins) emerge as previous infrastructure is dismantled. Recent crime reports note that while Bitcoin remains central to many darknet markets, a growing share of new platforms have shifted to **Monero-only** or privacy coin-preferred payment models, explicitly citing traceability concerns [6], [3]. This transition complicates longitudinal analysis, as flows may partially move off transparent blockchains or be fragmented across multiple assets and services.

In our framework, this behaviour can be interpreted as **temporal churn in the set of dominant intermediaries and routing strategies**: some chokepoints disappear under enforcement pressure, new ones appear, and the relative importance of different asset types (Bitcoin, stablecoins, privacy coins) changes over time.

D. Role-Specific Behavior of Markets, Mixers, and Exchanges

Prior labelled-entity studies indicate that different roles in the ecosystem exhibit **distinctive behavioural profiles**. Darknet markets typically act as large aggregation points, collecting many small inbound payments from users and periodically forwarding them to mixers or exchanges [11], [9]. Mixers, in contrast, are characterized by dense internal connectivity and patterns of splitting and recombining amounts designed to break simple traceability heuristics [12], [2]. Exchanges often function as terminal nodes for illicit paths, with inflows from multiple markets and services converging on a relatively small set of deposit clusters [9], [4].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, May 2026 Impact Factor: 8.2

Industry datasets and academic analyses jointly suggest that illicit-linked mixers and high-risk exchanges tend to receive **more volatile and geographically diverse inflows** than standard, regulated exchanges. Such behavioral distinctions support the use of role-aware tagging and feature-based profiling in monitoring systems: flows that traverse known market wallets, obfuscation services, and lightly regulated exchanges within a short time window are more likely to be associated with high-risk activity than flows confined to regulated entities and retail usage patterns.

E. Implications for Monitoring and Policy

Overall, the literature indicates that cryptocurrency usage in illegal markets exhibits **structural regularities** that can be exploited for monitoring and intervention:

Flows are **concentrated** in a small number of intermediaries, enabling focused disruption strategies.

Path structures from markets to exchanges are often **short and systematic**, supporting heuristic-based tracing.

Temporal behavior shows **observable reactions to enforcement**, revealing both vulnerabilities and adaptation patterns.

Different roles—markets, mixers, exchanges—have **distinct transaction-level signatures** that can be incorporated into risk scoring and anomaly-detection frameworks.

Our conceptual synthesis suggests that even without proprietary datasets, regulators, exchanges, and investigators can make use of public findings and tag lists to design**risk-based monitoring pipelines**. At the same time, the increasing migration of illicit flows toward privacy-enhancing technologies and alternative assets underscores the need for continued methodological innovation and cross-asset analysis in future work.

V. CONCLUSION AND FUTURE WORK

This paper examined how cryptocurrencies, particularly Bitcoin, are used within illegal markets by synthesizing prior empirical work on darknet ecosystems, laundering infrastructures, and transaction-graph analysis. Rather than constructing a full-scale transaction graph ourselves, we adopted a flow-oriented framework grounded in published datasets, address tag lists, and industry and academic measurement studies [11]–[4]. Within this framework, we discussed how value typically moves from darknet markets through mixers and high-risk exchanges, and how these flows are shaped by economic incentives and enforcement pressure.

Our review highlights several structural regularities in illicit cryptocurrency usage. First, flows linked to illegal markets tend to be highly concentrated in a small number of intermediary entities, creating potential chokepoints for regulatory and law-enforcement interventions [3], [12]. Second, path structures from markets to cash-out points are often relatively short, which both simplifies certain forms of tracing and motivates the use of obfuscation services such as mixers [5], [7], [2]. Third, illicit infrastructure displays temporal churn: enforcement actions and regulatory changes can significantly disrupt specific intermediaries, but flows may reappear through alternative services, privacy coins, and cross-asset routes [6], [3], [4]. Taken together, these findings underscore that illicit crypto activity is a minority of overall usage but remains operationally sophisticated and adaptive.

There are several directions for future work. A natural next step is to implement the full pipeline outlined conceptually in our methodology, using open transaction datasets (e.g., labeled Bitcoin graphs and public blockchain exports) to compute concrete flow metrics and validate them empirically. Extending the analysis beyond Bitcoin to include stablecoins and privacy-focused assets such as Monero would enable more comprehensive cross-asset comparisons of illicit routing strategies. In addition, integrating on-chain flow analysis with off-chain intelligence—such as marketplace forum data, sanction lists, and AML alerts—could support richer models of how criminal ecosystems respond to policy and enforcement changes. Finally, developing reproducible, open-source tools for flow-centric monitoring would help bridge the gap between academic measurement work and practical deployment in compliance, investigation, and regulatory settings.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

REFERENCES

[1] A. Trozze, S. A. Choo, L. T. Nguyen, and R. J. Broadhurst, "Cryptocurrencies and future financial crime," Crime Science, vol. 11, no. 1, 2022.
[2]Chainalysis, "Crypto Crime Report 2022," Chainalysis Inc., 2022. https://www.chainalysis.com [Online]. Available:
[3] D. Ron and A. Shamir, "Quantitative analysis of the full Bitcoin transaction graph," in Proc. 17th Int. Conf. Financial Cryptography and Data Security (FC), 2013, pp. 6–24.
[4] EMCDDA and Europol, EU Drug Markets: In depth Analysis of Darknet Markets, European Monitoring Centre for Drugs and Drug Addiction and Europol, Luxembourg: Publications Office of the European Union, 2022.
[5] F. Victor and A. Hagemann, "Multi-input clustering and the accuracy of Bitcoin transaction graph analysis," in Proc. Int. Conf. Financial Cryptography and Data Security Workshops (FC Workshops), 2021, pp. 1–10.
[6] H. T. Luong and D. A. Bright, "Preliminary findings of the trends and patterns of darknet markets," in Proc. 2022 IEEE Int. Conf. on Cyber Security and Resilience (CSR), 2022.
[7] J. Mariani and I. Homoliak, "SoK: A survey of mixing techniques and mixers for cryptocurrencies," arXiv preprint arXiv:2504.20296, 2025.
[8] K. Soska and N. Christin, "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem," in Proc. 24th USENIX Security Symp., 2015, pp. 33–48.
[9] M. Fleder, M. S. Kester, and S. Pillai, "Bitcoin transaction graph analysis," arXiv:1502.01657, 2015. arXiv
[10] N. Christin, "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace," in Proc. 22nd Int. World Wide Web Conf. (WWW), 2013, pp. 213–224.
[11] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: Characterizing payments among men with no names," in Proc. 2013 Internet Measurement Conf. (IMC), 2013, pp. 127–140.
[12] T. Moser, "Anonymity of Bitcoin transactions: An analysis of mixers," in Proc. Financial Cryptography and Data Security Workshops (FC Workshops), 2017, pp. 16–32.
[13] TRM Labs, Illicit Crypto Ecosystem Report 2024, TRM Labs Inc., 2024. [Online]. Available: