Unveiling the Shadows: Analyzing Cryptocurrency Address Management and Fund Movement of Darknet Markets

Aiman SYAZWAN BIN ABDUL RAZAK†, Yin MINN PA PA††, Katsunari YOSHIOKA†††, and Tsutomu MATSUMOTO†††

† Graduate School of Environment and Information Sciences, Yokohama National University

†† Institute of Advanced Sciences, Yokohama National University

††† Graduate School of Environment and Information Science, Institute of Advanced Sciences, Yokohama National University

E-mail: †aiman-razak-jm@ynu.jp, ††{yinminn-papa-jp,yoshioka,tsutomu}@ynu.ac.jp

Abstract Darknet markets use cryptocurrencies like Bitcoin for anonymous transactions in exchanging illicit goods and services. The restricted comprehension of cryptocurrency management and fund movements associated with darknet market impedes law enforcement, cybersecurity, and policy-making efforts to combat illicit activities in the darknet. To solve these problems, we focus on a two-fold approach, understanding cryptocurrency address management of darknet markets and the movement of funds within and outside of them. We study cryptocurrency address management by analyzing how darknet markets create Bitcoin addresses for invoices, exploring open-source darknet market frameworks on GitHub and their connections to darknet markets. Movement of funds within and outside of the darknet markets is traced by analyzing the Bitcoin transactions associated with addresses generated for market invoices.

Key words Darknet Market, Cryptocurrency, Address Management

1. Introduction

Darknet markets (DNMs) function as anonymous platforms facilitating the exchange of illicit goods and services, utilizing cryptocurrencies such as Bitcoin, Ethereum, and Monero to ensure transaction anonymity. By the end of 2022, the market revenue of cryptocurrency reached $1.5 billion[1]. Understanding trends in cryptocurrency address management within operational DNMs is crucial for law enforcement, cybersecurity, and policymaking efforts to combat illicit activities in the darknet.

However, the methods employed by DNMs to manage cryptocurrency addresses remain largely undisclosed, and addresses directly associated with these markets can potentially unveil the identities of those behind them. Therefore, we established three research questions to gain deeper insights into this issue:

RQ1. How do DNMs manage cryptocurrency address generation?
RQ2. How do DNMs and opensource DNM frameworks relate?
RQ3. What are the characteristics of cryptocurrency transactions generated by DNMs?

To address RQ1, we utilized both white-box and black-box methodologies. The white-box method involved analyzing internal details by accessing open-source DNM frameworks on platforms like GitHub. Additionally, employing the black-box method, we generated multiple invoices across various DNMs and analyzed the addresses they generated.

For RQ2, we conducted a comparison between the cryptocurrency address management systems identified through both the black box and white box approaches to evaluate their correlation. Additionally, we theorized that smaller markets tend to favor open-source frameworks because of resource limitations or convenience. To investigate this, we conducted a market scale analysis, categorizing DNMs based on factors such as product diversity, operational longevity, and presence on ranked listings in surface websites. Subsequently, we analyzed this data to determine whether there is a tendency for small and large DNMs to adopt specific cryptocurrency address management systems. For RQ3, we examined cryptocurrency transactions associated with addresses obtained from invoices using both blockchain explorer[2] and wallet explorer[3] to trace fund flow.

Our investigation revealed:

(1) 7 types of cryptocurrency address management systems implemented in open-source frameworks and DNMs.
(2) 2 out of 4 of the cryptocurrency address management systems identified through the white box approach align with those implemented by the DNMs identified through the black box approach.
(3) We identified the trends in implemented cryptocurrency address management systems within small and large DNMs. Compared to other cryptocurrency address management systems, the practice of generating a new address for each order is widely adopted across both small and large DNMs.
(4) Recurrence of certain common addresses, associated with substantial funds, across multiple darknet markets, suggesting the presence of a common service within the darknet.
(5) The repeated appearance of certain common wallets with minimal funds across various DNMs, all tracing back to the same exchange platform, Binance[4], suggests the possibility that these wallets belong to a vendor or operator who utilizes multiple DNMs.

2. Background

2.1 Darknet

The darknet is a part of the Internet inaccessible through conventional search engines, operates on overlay networks that demand specific software, configurations, or authorization for access. Within the darknet, individuals engage in various online activities, both legal and illegal, beyond the confines of traditional online spaces. It serves as a platform for communication, information sharing, and transactions that often prioritize anonymity. The darknet encompasses networks like TOR, alongside various others, each tailored to specific functionalities and user demographics. For example, accessing the TOR network can be done through a TOR Browser[5] or an Onion Proxy when using a standard surface web browser. The TOR Browser prioritizes users' privacy and anonymity[6]. As users browse the internet via the TOR Browser, their connections traverse a series of volunteer-operated servers, known as relays[7]. At each relay, a layer of encryption is decrypted, unveiling the subsequent relay in the route. This layered routing process, akin to peeling back the layers of an onion, epitomizes the core concept behind "The Onion Router".

2.2 Darknet Market & Illicit Transactions

Darknet markets (DNMs) are online platforms within the darknet that facilitate the exchange of goods and services, often illicit or illegal. These markets operate on a model similar to e-commerce platforms, allowing users to browse products, read reviews, and make purchases. Cryptocurrencies such as Bitcoin, Ethereum, and Monero are the primary means of payment within DNMs. The decentralized nature of cryptocurrencies enables users to make transactions without the need for traditional banking channels, offering a higher level of privacy and security. The pseudo-anonymous nature of cryptocurrency transactions aligns with the anonymity sought by participants in darknet activities.

2.3 Purchasing & Payment Process in Darknet Market

The buyer navigates a catalogue of prohibited goods and services, selecting items that are then added to a virtual cart, similar to e-commerce platforms on the surface web. Upon proceeding to checkout, the DNM generates an invoice that details the total amount owed, a breakdown of individual items with associated costs, and a crucial payment address. This payment address, an alphanumeric string linked to the transaction, serves as the means for cryptocurrency payments. Using the privacy features inherent in cryptocurrencies such as Bitcoin, Ethereum, or Monero, the buyer transfers the required funds from their wallet to the provided address, finalizing the transaction. The confirmation of payment on the blockchain prompts the darknet market to acknowledge the successful transaction, after which sellers may provide additional instructions for product delivery or access. This payment process leverages the anonymity of TOR and cryptocurrencies to safeguard the identities of both buyers and sellers engaged in these illicit transactions.

2.4 Blockchain Forensics Tools

2.4.1 Blockchain Explorer

A blockchain explorer[2] is an online tool that grants users access to interact with data on a blockchain network. It facilitates the viewing of transactions, addresses, blocks, and other pertinent information recorded on the blockchain. With blockchain explorers, users can easily track and verify transactions, as well as delve into the history and current status of the blockchain network, thus providing transparency and visibility into its operations. These tools are indispensable for gaining insights into the activity and dynamics of blockchain networks.

In the realm of blockchain forensics, blockchain explorers play a pivotal role. This field involves examining blockchain data to uncover patterns, trace transactions, and identify entities engaged in illicit activities such as money laundering or fraud. By harnessing blockchain explorers, forensic investigators gain access to detailed transaction records, addresses, and blocks, empowering them to track fund flows, pinpoint suspicious transactions, and trace asset movements across the blockchain network.

Utilizing blockchain explorers, investigators can compile evidence, establish connections between various addresses or entities, and reconstruct transaction histories. These tools are crucial for conducting comprehensive investigations, aiding law enforcement agencies, regulatory bodies, and other stakeholders in combating financial crimes within the blockchain ecosystem.

2.4.2 Wallet Explorer

A wallet explorer[3] is a tool or service, like WalletExplorer.com, that allows users to explore and interact with data on the Bitcoin blockchain. In addition to basic blockchain explorer features, WalletExplorer.com has two unique functionalities:

It merges addresses together if it determines that they are part of the same wallet. It allows wallets to have names. WalletExplorer.com computes wallets using a basic algorithm based on co-spending transactions. If addresses A and B are co-spent in one transaction, and addresses B and C are co-spent in another transaction, all addresses A, B, and C are considered part of the same wallet. However, if an address has not been co-spent with others, it remains unnamed. Names for wallets are discovered by registering to services, making transactions, and observing which wallets the bitcoins are merged with or withdrawn from. A wallet ID is an identifier generated by WalletExplorer.com, typically in hexadecimal format. It is derived from an MD5 hash with a static salt, often representing the lowest hash among multiple addresses within a wallet. The first 8 bytes (16 alphanumeric characters) of the hash serve as the identifier, with the remaining 6 characters (3 bytes) used for color differentiation. These colors are purely visual aids and have no functional significance outside of WalletExplorer.com.

3. Methodology

Our investigations were conducted from May 9, 2023 to January 9, 2024. We employed 4 approaches to address the following research questions:

RQ1. How do DNMs manage cryptocurrency address generation?
RQ2. How do DNMs and opensource DNM frameworks relate?
RQ3. What are the characteristics of cryptocurrency transactions generated by DNMs?

To address RQ1, we utilized both white box and black box approaches, which are elaborated in detail in Sections 3.1 and 3.2, respectively. The white box approach involves utilizing GitHub's search engine to identify repositories related to DNMs. We focused on backend aspects, analyzing blockchain integration, payment gateways and address/invoice generation methods. In the blackbox approach, we manually navigated the darknet using search engines like Ahmia[4] , Torch[5], and Deep Search[6] . Forums like Dread[7] and surface websites listing DNM URLs were investigated. We selected products across various categories to explore cryptocurrency address management system variations. This involved repeatedly generating invoices to investigate address occurrence rates. It's crucial to emphasize that all addresses collected in this research are bitcoin addresses, and no other cryptocurrencies were considered. Blockchain explorer[2] and wallet explorer[3] were used to analyze payment addresses and cluster addresses from the same wallet.

For RQ2, we compared the cryptocurrency address management systems identified through both the black box and white box approaches to assess the likelihood of DNMs implementing open-source frameworks. Additionally, we conducted a market scale anal-

ysis, as detailed in Section 3.3, by examining the range of products offered by DNMs to evaluate the trends in cryptocurrency address management system implementation. In this research, a large DNM is one with 4 or more product categories, while a small DNM has 3 or fewer product categories.

To address RQ3, we conducted a fund movement analysis, the details of which are explained in Section 3.4. This analysis focused on cryptocurrency inflow, internal movement within the market, and outflow. Transaction volumes were compared with product prices, and temporal aspects were considered. Wallet IDs were cross-referenced using a wallet explorer to identify common wallets and addresses.

3.1 White Box Approach

The keyword "Darknet Market" is employed in GitHub's search engine in May 2023. Subsequently, we manually examined all files within related repositories to identify any web applications or frameworks relevant to DNMs. Our focus primarily centered on the backend aspects, analyzing the cryptocurrency address management systems within these repositories. We manually examined source code related to payment gateways, address and invoice generation, as well as buyer and vendor accounts to determine if addresses were generated for every order, account, or other methods.

3.2 Black Box Approach

In our research, we manually navigate the darknet using search engines like Ahmia[4], Torch[5], and Deep Search[6], specifically to find DNM URLs. We further investigate Dread, a prominent forum within the darknet community, along with surface websites that list darknet market URLs.

Upon gaining access to these markets manually, we meticulously choose products spanning diverse categories, including drugs, firearms, malware, leaked data, and cryptocurrency address private and public keys. This selection allows us to explore the potential variations in cryptocurrency address management system associated with each product category. This checkout process is repeated up to a maximum of 10 times for every market to collect bitcoin addresses and investigate the address's occurrence rate.

To investigate whether the generated address is used or unused, a blockchain explorer[8] is employed to examine past transactions associated with it. Additionally, we utilize a wallet explorer[9], a system that clusters addresses from the same wallet. This system aids us in investigating whether the addresses generated in several invoices is generated by one or more wallet.

3.3 Market Scale Analysis

We conducted an analysis of market scale by investigating the range of products offered by DNMs to gain insight into their scope. The product categories encompassed cryptocurrency public and private keys, credit cards, money transfers, drugs, firearms, hacking services, digital devices, leaked data, and fake documents. In this study, we define a large DNM as those with 4 or more product categories, whereas a small DNM is characterized by having 3 or fewer product categories. However, it's essential to note that a comprehensive understanding of market scale would ideally include additional front-end analysis such as evaluating the number of listings, seller reputation, transaction volume, geographical coverage, product diversity, and platform features. Unfortunately, due to time constraints, we were only able to focus on assessing the product range.

3.4 Fund Movement Analysis

In Section 3.2, we clarified the methodology for collecting multiple addresses directly associated with the market by repeatedly generating invoices.

Subsequently, we executed a transaction analysis for bitcoin addresses with past transactions. The cryptocurrency tracing process is systematically categorized into three distinct movements: cryptocurrency inflow into the market, internal cryptocurrency movement within the market, and the outflow of cryptocurrency from the market. Throughout the tracing process, consideration is given to whether the transaction volume aligns with the market's product prices, and the temporal aspects of each transaction are also considered to uphold trace integrity.

When tracing Address A obtained from a DNM, we distinguish between incoming and outgoing transactions. Incoming transactions are examined to analyze funds entering the market, while outgoing transactions are examined to track funds leaving the market. Internal transactions, denoted by addresses sharing the same wallet ID as identified via wallet explorer[3], are also noted. In the case of analyzing an outgoing transaction for address A, the timestamp of the latest transaction for address A is logged as the starting point for the trace. This timestamp serves as the limit when examining transactions on a different address while increasing the depth for this particular trace.

Additionally, we cross-referenced wallet IDs via a wallet explorer[3] for every address involved in the transactions to identify common wallets and addresses across all traces. We concluded the trace upon encountering signs of mixing, such as transactions involving input or output addresses from 20 or more wallets. This decision was driven by the manual process of conducting the trace, which made it challenging to track all addresses from all wallets. However, if the input or output addresses of a certain transaction originate from the same wallet, indicating no mixing, the trace is continued until reaching an address with a transaction volume exceeding $10,000,000,000, indicating involvement with an exchange platform.

4. Result

RQ1. How do DNMs manage cryptocurrency address generation?
RQ2. How do DNMs and opensource DNM frameworks relate?
RQ3. What are the characteristics of cryptocurrency transactions generated by DNMs?

For RQ1, both the black box and white box approaches identified a total of 8 systems for managing cryptocurrency address generation as explained in Section 4.1.1.

For RQ2, from the white box approach, we found 4 cryptocurrency address management systems, with 2 of them being implemented by DNMs identified in the black box approach. Large DNMs numbered 15, while small ones were 42 as described in Section 4.2.2. Across both categories, the most common practice was to generate a new address for each new order, indicating its widespread popularity. Small DNMs, however, tended to favor using the same address for every invoice, possibly due to a preference for simplicity and efficiency.

Meanwhile for RQ3, the fund movement analysis provided insights into the usage of common addresses and wallets, as well as DNM revenue. Further details regarding each cryptocurrency address management system, common address, common wallet, and DNM revenue are explained in Section 4.3.

4.1 Cryptocurrency Address Management Systems

4.1.1 Black Box & White Box Approach

A total of 8 cryptocurrency address management systems were identified using both white box and black box methods, each defined and labeled as shown in Table 1:

Cryptocurrency address management system A involves generating a new address for each new order made by the buyer. Cryptocurrency address management system B entails including one address from one or multiple wallets in the invoice when an order is placed. Cryptocurrency address management system C generates the same address for every invoice associated with each order. Cryptocur-

Table 1 Description of all cryptocurrency address management system(CAMS) identified

CAMS	Description
A	New Address/Order
B	One Address from Wallet/Order
C	Same Address/Order
D	New Address/Account
E	One Address from Wallet/Account
F	One Address/Item
G	Lightning Payment
H	Wallet/Account

rency address management system A to C require the buyer to send funds directly to the generated address, which will subsequently be confirmed on the blockchain.

Cryptocurrency address management system D involves generating one address for every account created on the market's platform. Cryptocurrency address management system E involves including one address from the same or multiple wallets, sourced from the Wallet ID provided by wallet explorer[3], for every account created on the market's platform. Addresses in systems D and E function as deposit addresses, with funds used to purchase products directly from the market. Any remaining funds can also be withdrawn. Cryptocurrency address management system F ties every item on the market to a single address. Cryptocurrency address management system G refers to lightning payment, a layer 2 Bitcoin protocol. Lightning Network enables instant transactions between participating nodes and has the capability to significantly reduce transaction fees and increase scalability of the Bitcoin network. Cryptocurrency address management system H allows an account of the market to generate multiple addresses.

Addresses generated in systems A and D cannot be classified or clustered to determine whether they originate from the same or different wallets using wallet explorer[3]. However, addresses generated in systems B, C, E, and F can be clustered to identify the wallet of origin via wallet explorer[3]. Furthermore, Cryptocurrency address management system G and H are exclusively observed in frameworks identified through the white box approach.

4.1.2 White Box Approach: Cryptocurrency Address Management System of DNM Open-Source Frameworks

A total of 8 repositories were identified in GitHub hosting full-stack web applications of DNMs. However, upon closer inspection, it was evident that 4 of these repositories were outdated and incomplete, thereby necessitating exclusion from our analysis. The remaining 4 repositories that underwent thorough examination include TradeMed[9], OpenBazaar[10], SqueakRoad[2211], and Eckmar[12]. The cryptocurrency address management system implemented in each respective framework can be seen in Table 2.

Table 2 Open-Source Frameworks' cryptocurrency address management systems(CAMS)

Framework	CAMS
TradeMed	A
OpenBazaar	D
Eckmar	H
SqueakRoad	D + G

4.1.3 Black Box Approach: Cryptocurrency Address Management System of DNM

From the 58 DNMs we examined, we identified 7 cryptocurrency address management systems by analyzing the generation of multiple invoices and their associated addresses. However, we were unable to identify one cryptocurrency address management system implementation. This happened because some addresses generated in the invoices had past transactions associated with them, while others did not. Additionally, the addresses with no past transactions could not be identified by wallet explorer[3]. This complicates the assessment of how the DNM manages both its used and unused addresses. Table 3 provides details on the total number of DNMs using each payment system, as well as DNMs with transaction history(w) and those without transaction history(w/o).

Table 3 Address Transaction History & DNM cryptocurrency address management system (CAMS)

No. of DNM		
w	w/o (Past Transactions)	CAMS
0	37	A
4	0	B
8	0	C
0	6	D
1	0	E
1	0	F
1	0	Unidentified

4.2 Black Box Approach & White Box Approach Correlation

4.2.1 Cryptocurrency Address Management Systems Identified in DNMs & Open-Source DNM Frameworks Relationship

The correlation between the black box and white box methods lies in their combined efforts to gain a comprehensive understanding of the DNM. While the black box method involves direct exploration of the darknet through manual navigation and observation of its functionalities, the white box method delves into the underlying infrastructure and code base of DNM frameworks found on platforms like GitHub.

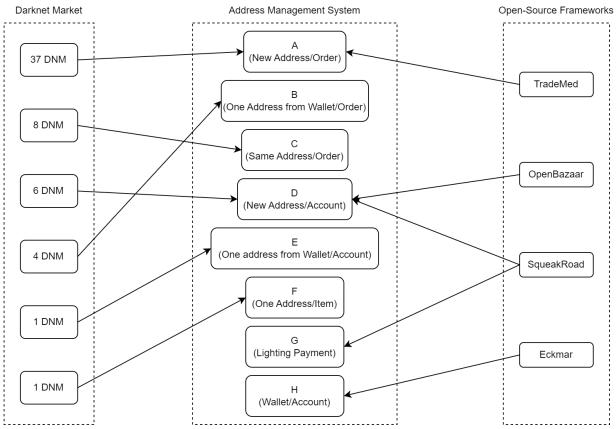
The correlation between these methods becomes apparent when we aim to bridge the gap between the observed behavior of DNMs in the black box method and the underlying mechanisms identified through the white box method. Specifically, leveraging the findings from the white box method allows us to determine which active DNMs employ the cryptocurrency address management system identified in our analysis. By correlating the cryptocurrency address management system identified through the black box method with the cryptocurrency address management system and frameworks identified in the white box method, we can better understand how addresses are generated, managed, and utilized across different DNMs as illustrated in Figure 1.

However, further analysis of the front-end of live DNMs and the frameworks is needed to accurately determine whether any of them actually utilize the frameworks identified through the white box method. This analysis would involve examining the user interface, features, and functionalities of live DNMs to identify any correlations with the frameworks' characteristics identified in our study. By conducting this additional investigation, we can validate our initial findings and provide more robust insights into the utilization of these frameworks within the darknet ecosystem.

4.2.2 Market Scale Analysis & Cryptocurrency Address Management System Relationship

The number of DNMs with product categories ranging from 1 to 9 is presented in Table 4. In this research, a large DNM is defined as DNMs with 4 or more product categories, while a small DNM is defined as DNMs with 3 or fewer product categories. Using the

Fig. 1 Cryptocurrency address management system implemented in open-source frameworks & DNM

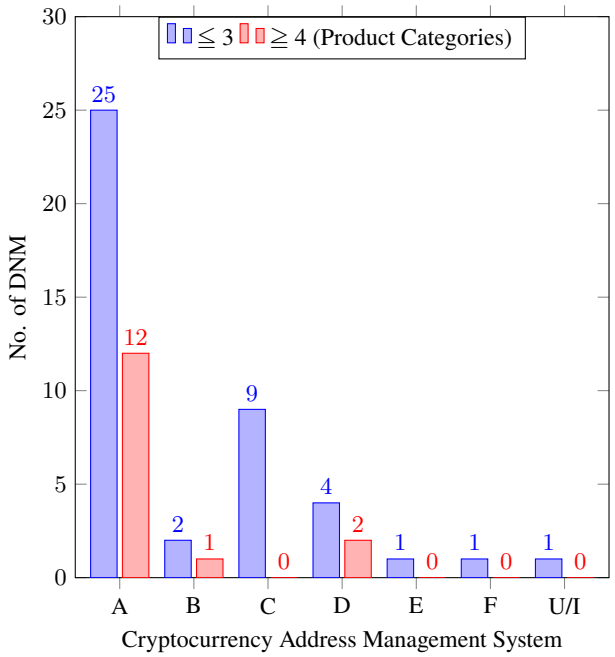


data on each DNM's cryptocurrency address management system implementation, the trend of smaller and larger markets and their preference for specific types of cryptocurrency address management system can be analyzed.

Table 4 Distribution of DNMs by Number of Product Categories

Size	No. of product categories	No. of DNM
Small DNMs	1	28
	2	8
	3	7
Large DNMs	4	4
	5	5
	6	4
	7	0
	8	2

Fig. 2 Distribution of DNM by scale & cryptocurrency address management system



Cryptocurrency address management system A, involving the generation of a new address for each new order, is the most commonly implemented system across both small and large DNMs, indicating its widespread adoption and popularity.

Cryptocurrency address management system C, generating the same address for every invoice associated with each order, appears to be more prevalent in small DNMs compared to large DNMs, suggesting a potential preference for simplicity and efficiency in address management among smaller markets.

Large DNMs, demonstrate a diverse preference for cryptocurrency address management system, with 12 implementing cryptocurrency address management system A and 2 implementing cryptocurrency address management system D, while only 1 implements cryptocurrency address management system B. This preference for systems A and D among larger DNMs, as well as across all DNMs, implies a heightened concern for anonymity levels, as discussed in Section 5.1, compared to smaller markets.

4.3 Fund Movement Analysis

A total of 129 bitcoin addresses were recorded from 58 DNMs, with 19 addresses from 10 markets identified. However, only traceable addresses from 6 out of these 10 markets were traced due to time constraints. These traces revealed DNM market revenue and identified multiple common addresses and wallets.

4.3.1 Common Address & Wallet

All addresses listed in Table 5 have a volume exceeding $10,000,000,000. Volume represents the total amount of money sent and received by an address. They're also strategically positioned either at the beginning or end of the tracing results due to the significant number of transactions associated with them. This suggests a pattern that these addresses serve a common purpose in the darknet. They could function as hubs for a popular exchange platform utilized by Darknet Market users, facilitating discreet money transfers. This observation hints at a concealed network where specific addresses play pivotal roles in enabling illicit transactions. Address 6 and 7 in Table 5 are verified to be two of Binance's addresses. Furthermore, address 3 and 4 have been associated with scam reports on Bitcoin's "Who's Who" registry[8][9]. Further analysis could unveil more about their significance and impact on the darknet economy.

Two distinct addresses in Table 6 sharing the same wallet ID were recorded from two separate markets. One market specializes in selling social media hacking services, while the other market deals in the sale of credit cards. Notably, both address exhibited low transaction volume, with a total sent and received value exceeding $5000. The positions of both of these addresses were traced outside of the market, meaning that they were identified after a depth of 4 and 6, respectively, without any association with the addresses collected directly from the market itself and before any exchanges or addresses with large transaction volumes, as observed in Table 5. Moreover, both addresses consistently directed almost all funds received to the same destination address, "bc1qw-3qc77", which ultimately leads to Binance. Such patterns prompt speculation regarding the possible identity of the wallet holder. It's plausible that the wallet holder operates as a vendor across various platforms, aiming to consolidate earnings efficiently. Alternatively, they could be an operator overseeing multiple markets.

4.3.2 DNM Revenue

The address was extracted from the Dumps Market, a DNM specializing in the sale of Bitcoin public and private keys. This market utilizes a single address for every order placed. Our investigation of this market concluded in June 2023, revealing 218 transactions associated with the address at that time. Among these transactions, 125 out of 218 were precisely matched to the market's listed item prices, enabling the calculation of the revenue generated by this market. The total amount of BTC received in these 125 transactions summed up to 0.1275 BTC, equivalent to approximately $6600.89

Table 5 Traced address & source of DNM

		DNM				
No.	Address	Market 1	Market 2	Market 3	Market 4	Market 5
1	bc1qa-w688k	✓				
2	bc1q7-zpemf	✓		✓	✓	
3	bc1q8-0syvz		✓	✓	✓	
4	bc1qx-pm79r		✓	✓	✓	
5	bc1qn-pju8q	✓				
6	1NDyJ-obu1s (Binance)		✓	✓	✓	
7	bc1qm-77s3h (Binance)		✓	✓		
8	bc1qq-cfvgq	✓				✓

Table 6 Common Wallet in Multiple Traces

Wallet ID	Address	Source
000842a323	3FBkq-71mHV	Market 3
	3Jqwu-kZdLP	Market 4

based on the exchange rates on February 20, 2024. The frequency of transactions that match the item prices on the website can be observed in Table 5 below.

Table 7 Frequency of transactions that matches the price of product

Item Price (BTC)	Frequency of transactions
0.01200	1
0.00600	1
0.00400	5
0.00350	3
0.00200	15
0.00100	46
0.00050	51
0.00025	3

5. Discussion

5.1 Anonymity of DNM based on Cryptocurrency Address Management System

The anonymity level of DNM users varies depending on the cryptocurrency address management system implemented. In Table 3, it is observed that out of a total of 37 DNMs implementing cryptocurrency address management system A, and 6 DNMs implementing cryptocurrency address management system D, none have associated addresses with past transactions. Conversely, DNMs utilizing other cryptocurrency address management system display addresses with past transactions in their invoices. This discrepancy could significantly impact the anonymity level of the market, as addresses with past transactions could be directly linked to it. Further analysis of these transactions could uncover additional services that are commonly used in the darknet, potentially revealing the identity of vendors/operators and shedding light on revenue streams, thereby providing insight into the DNM ecosystem as shown in Sections 4.3.1 and 4.3.2.

5.2 Implications of Common Addresses and Wallets

The identification of common addresses across multiple DNMs, particularly those associated with substantial funds, raises questions about the underlying infrastructure supporting illicit transactions. The recurrence of certain addresses suggests the presence of common services or exchange platforms utilized within the darknet. Furthermore, the discovery of common wallets linked to the same exchange platform, such as Binance, hints at the possibility of centralized operations or vendor activities spanning multiple markets. This finding highlights the interconnected nature of darknet transactions and the potential challenges for law enforcement in tracking illicit fund flows.

5.3 Revenue Tracking and Market Insights

The study's approach to correlating transactions with corresponding product prices on DNMs offers a accurate method for estimating market revenue and understanding transaction patterns. By analyzing transaction volumes and identifying matches with listed item prices, researchers gain valuable insights into market dynamics and revenue streams. This information not only enhances our understanding of the darknet economy but also provides actionable intelligence for law enforcement agencies seeking to disrupt illicit activities.

5.4 Bridging White Box and Black Box Methods in DNM Research

The study's methodology, which combines white box and black box approaches, underscores the multifaceted nature of investigating darknet markets. While the white box approach provides insights into underlying frameworks and infrastructure, the black box approach offers firsthand observations of market operations and user behaviors. This methodology diverges from conventional research on DNMs, which typically revolves around data scraping and analysis.

6. Related Work

Research efforts have been directed towards comprehensively understanding the operations of DNM since the emergence of Silk Road. Research by Maras delved into the operations and features of Silk Road [14], offering valuable insights into its functioning as a prominent Darknet marketplace. Maras's work shed light on Silk Road's role as a platform for illicit trade, including the sale of drugs, counterfeit documents, and hacking tools. Additionally, Maras explored Silk Road's use of privacy-enhancing technologies like TOR Browser[5] and tumblers to maintain anonymity for its users. This research provided a foundational understanding of the operational dynamics and characteristics of Silk Road, contributing to the broader comprehension of Darknet markets. Georgoulias et al.[15] contributed to understanding the features and operations of DNMs[15]. Their work focused on mapping the infrastructure of 41 marketplaces, 35 vendor shops, and 3 independent forums within the darkweb ecosystem. While both studies shed light on "on-site wallets", specific to cryptocurrency address management system D mentioned in Section[4.1.1], they did not explore other types of address management systems, highlighting the need for further investigation into the diversity of address management practices within DNMs.

Matthew Ball[16] proposed a method that addresses these chal-

lenges by employing both quantitative and qualitative analyses. They describe the products listed, sale volumes, prices, and quantities sold on particular markets, as well as examine the impact of law enforcement actions or cyberattacks on market diversity and user/vendor behavior. Furthermore the study on White House Market [17] developed automatic captcha solvers for object recognition and puzzle captchas, achieving accuracy rates of nearly 78% and 83%, respectively. By integrating these into their architecture, they successfully crawled the marketplace gathering comprehensive data on product types, vendor statistics, and vendor behavior on other platforms. They also extracted valuable insights from PGP public keys, revealing key reuse patterns and popular email providers among vendors.

However, Cuevas et al.[18] underscored the challenges of relying solely on frontend scraping to estimate market revenue. Their study revealed potential biases in revenue estimates, emphasizing the importance of considering measurement accuracy. Such methods may underestimate market metrics due to missed market activity. In our study, we proposed a method to calculate a DNM revenue using the black box approach and fund movement analysis as described in Sections 3.2 and 3.4 respectively, offers an alternative to frontend scraping for a more accurate revenue estimation.

The techniques discussed in Tin et al.[19] primarily revolve around address taint analysis and backward address tainting to trace the flow of funds within the Bitcoin transaction network. These methodologies, coupled with the application of filtering criteria to mitigate false positives, significantly contribute to the overarching objective of tracking mixer services and comprehending fund flows within the Bitcoin ecosystem. However, Tin et al. also highlighted the potential limitation of relying on external information, as inaccuracies from unreliable sources could lead to misinterpretations of illicit activities. This underscores the importance of exercising caution when integrating external data into blockchain forensics analyses, emphasizing the necessity for thorough verification and validation of external sources to ensure the accuracy and reliability of the findings.

Furthermore, if these techniques were applied to addresses directly obtained from DNMs, it could provide richer characteristics and insights. Unlike mixed funds datasets, addresses from DNMs offer clearer contexts and potential connections to illicit activities within the darknet ecosystem. Analyzing these addresses with blockchain forensics methods could yield valuable insights into fund flows, transaction patterns, and identify illicit actors more precisely. This approach has the potential to enhance our understanding of illicit activities within DNMs and bolster law enforcement efforts in combating such activities.

In comparison to previous studies, this research endeavors to bridge the gap between white box and black box methodologies in investigating DNMs. While earlier studies often focused on singular aspects such as market operations or user behaviors, this study adopts a multifaceted approach, integrating insights from both the underlying infrastructure of DNM frameworks and firsthand observations of market operations. By combining these methodologies, this research provides a more comprehensive understanding of the intricate landscape of cryptocurrency address management within DNMs. Moreover, while previous studies may have overlooked certain aspects of address management practices or relied solely on frontend scraping for revenue estimation, this study employs techniques such as fund movement analysis to unravel illicit financial activities within DNMs. Thus, this research not only contributes to filling gaps in existing literature but also sets a precedent for future studies seeking to explore the complex dynamics of darknet markets more comprehensively.

7. Limitation & Future Work

The study faced challenges in accessing a comprehensive dataset of DNM links, limiting the depth of analysis on cryptocurrency address management practices. Additionally, the focus on a limited number of frameworks may have overlooked alternative applications used in DNMs, while the lack of a comprehensive analysis of front-end interfaces hindered the validation of research findings. Moreover, the study solely examined Bitcoin address management, neglecting other cryptocurrencies commonly used in DNMs, which could have provided a more nuanced understanding of address management practices. Market scale analysis is hindered by limited data availability and a narrow scope, suggesting the need for additional data to be included in the analysis for a more accurate understanding of DNM scale. Furthermore, the fund movement analysis was constrained by the detection of mixing, limiting the understanding of illicit financial activities within DNMs. Future research could explore alternative methods to gather a broader dataset of DNM links, conduct thorough front-end analyses, broaden the scope to include diverse cryptocurrencies, and employ advanced tracing techniques to unravel the movement of mixed funds, thus enriching the understanding of cryptocurrency address management and DNM dynamics. One notable limitation of this study is the reliance on manual analysis for both black box and white box approaches, as well as tracing the fund movement manually.

8. Conclusion

In conclusion, this study sheds light on the intricate landscape of cryptocurrency address management within DNMs. By investigating address generation methods, market scales, and fund movement, valuable insights have been gained into the mechanisms underpinning illicit transactions. However, limitations in data access, tracing methods, and framework analysis highlight areas for future research. By embracing advanced techniques, broadening the scope to include diverse cryptocurrencies, and delving deeper into market dynamics, future studies can contribute to a more comprehensive understanding of illicit activities in darknet markets, aiding efforts in law enforcement, cybersecurity, and policy-making.

Acknowledgement: Part of this study was supported by JSPS research grant 22H03588.

References

[1] Chainalysis, (2023, February 9), "How Darknet Markets and Fraud Shops Fought for Users In the Wake of Hydra's Collapse", https://www.chainalysis.com/blog/how-darknet-markets-fought-for-users-in-wake-of-hydra-collapse-2022/
[2] https://www.blockchain.com/explorer
[3] https://www.walletexplorer.com/
[4] ahmia.fi
[5] torchdeedp3i2jigzjdmfpn5ttjhthh5wbmda2rr3jvqjg5p77c54dqd.onion
[6] search7tdrcvri22rieiwgi5g46qnwsesvnubqav2xakhezv4hjzkkad.onion
[7] g66ol3eb5ujdckzqqfmjsbpdjufmjd5nsgdipvxmsh7rckzlhywlzlqd.onion
[8] https://www.binance.com
[9] https://www.torproject.org/
[10] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 482–494, 1998
[11] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second generation onion router", Naval Research Lab Washington DC, Tech.Rep., 2004
[12] bitcoinwhoswho.com/address/

bc1qx65xcxz6dfsge2g4eaererc slh83y66wrpm79r
[13] bitcoinwhoswho.com/address/
bc1q8yja3gw33ngd8aunmfr4hj820adc9nlsv0syvz
[14] https://github.com/B0bbyB0livia/trademed
[15] https://github.com/OpenBazaar
[16] https://github.com/yzernik/squeakroad
[17] https://github.com/eckmarcommunity/eckmar
[18] Maras, Marie-Helen, ”Inside Darknet: the takedown of Silk Road”, Criminal Justice Matters, 98(1):22-23, 10.1080/09627251.2014.-984541, October 2014
[19] Georgoulias, Dimitrios, Pedersen, Jens, Falch, Morten, Vasilomanolakis, Emmanouil. ”A qualitative mapping of Darkweb marketplaces”, 10.1109/eCrime54498.2021.9738766, 2021
[20] Matthew Ball, Roderic Broadhurst, ”Data Capture and Analysis of Darknet Markets”, February 18, 2021.
[21] York Yannikos, Julian Heeger, Martin Steinbach, ”Scraping and Analyzing Data of a Large Darknet Marketplace”, Journal of Cyber Security and Mobility, May 2023.
[22] Alejandro Cuevas, Fieke Miedema, Kyle Soska, Nicolas Christin, Rolf van Wegberg, ”Measurement by Proxy: On the Accuracy of Online Marketplace Measurements”, USENIX 2022
[23] Tin Tironsakkul, Manuel Maarek, Andrea Eross, Mike Just, “Tracking Mixed Bitcoin”, September 29, 2021