The Influence Of Technological Factors On Dark Web Marketplace Closure

Michael Kyobe and Hishaam Damon

Abstract—**The Dark Web serves as a platform to enable a host of illegal cyber activities. One such activity is Dark Web Marketplaces that operate as e-commerce websites but facilitate the sale of illicit goods and services. Various government and law enforcement agencies have surged many resources in trying to reduce dark web marketplace-related cybercrime. Still, dark web users can set up new marketplaces that become even more demanding to infiltrate. This study aimed to understand the influence of technological factors on dark market closures and how this could aid government and law enforcement in responding to dark web marketplace challenges quicker. Literature was synthesized to identify key technological factors that influence marketplace operations. These were: Anonymization, cryptocurrencies, decentralization, and codebase. A conceptual model was then developed and analyzed using quantitative data compiled from 87 dark web marketplaces. The findings suggest each of the technological factors identified has a low likelihood of influencing marketplace closures.**

Keywords; Dark Web Marketplaces, Cybercrime, Online Anonymity, Law Enforcement, Technological Factors

I. INTRODUCTION

There are three layers to the internet. The first layer, the Surface Web, has been extensively crawled and indexed and is accessed through common browsers such as Google, Firefox, and Microsoft Edge [1]. Despite its assumed size, the surface web only accounts for approximately five percent of all the information accessible on the World Wide Web. The other ninety-five percent of information is situated on the second layer, commonly referred to as the Deep Web [2]. The Deep Web has not been extensively crawled or indexed by search engines, such as Google, meaning all the information on it is inaccessible to the public and can only be accessed by navigating to a specific internet address [3]. The Deep Web contains primary harmless and protected data such as a university intranet system or information from password-protected websites such as banking details [4].

Growing expeditiously within the Deep Web is the third and final layer to the internet known as the Dark Web or, as some refer to it, the Darknet (1). A unique web browser is required for users to access the Dark Web. The most popular of these web browsers is The Onion Router (TOR) which provides anonymity to its users through redirecting internet traffic [5]. Various illegal activities take place on the Dark Web. The present study focuses on Dark Web Marketplaces, also referred to as Dark Marketplaces and the technological factors that enable them.

A significant concern regarding Dark Web Marketplaces is surrounding regulation. As the Dark Web is part of the world wide web, which is information sharing across multiple borders, it is difficult for specific governments to regulate international activity. In addition, because of the wide range of use cases that the deep web facilitates, simply restricting access is unfeasible (6). Much to the dismay of law enforcement, the closure of Silk Road, the largest Dark Web marketplace to date, had little to no effect on curbing cybercrime, and the economy of the Dark Web (7) Dark Web marketplace revenue was estimated to have increased by two hundred million USD since 2019, going from 1.3 billion USD to 1.5 billion USD in 2021. Dark Web marketplaces are anticipated to become more user-friendly and inventive, and the marketplace aspect is expected to increase as customer demand increases (8). Darknet users continue to establish new marketplaces that become more challenging to penetrate (9). (8) stated that the Darknet would become even more problematic to infiltrate as technology advances.

Thus, the purpose of this research is to determine the influence of technological factors on dark market operations, describe better how dark markets operate and allow for formulation of appropriate regulations and assist in the broader strategy of trying to detect, intercept and respond to illegal dark market activity (1).

II. LITERATURE REVIEW

Dark Web Marketplaces are built off the idea of eCommerce and function like the Alibaba Group or eBay but differ in the strong anonymity they offer their users. This vital anonymity aspect can be attributed to the web browsers needed to access these marketplaces and the cryptocurrencies that finance transactions [10]. Dark Web marketplaces offer an extensive range of products, the most frequent being illegal goods such as drugs, malware, and weapons [11]. The anonymity component provided with Dark Web marketplaces is used to elude law enforcement [12]. There are currently forty-four (44) Dark Web marketplaces active as of the beginning of 2021. Some of these marketplaces include the third installment of the original Silk Road, called Silk Road 3.1, and the DarkFox Market, which is currently one of the largest marketplaces in 2021 [14]. In addition, since the covid-19 pandemic, Dark Web marketplaces have witnessed an increase in bulk buying from users and the sale of personal protective equipment (PPE) and other medical goods [15]. them. However, in the context of this paper, online anonymity will extend to the technological aspect in which online activity cannot be linked to an Internet Protocol (IP) address [17]. Simply hiding your identity over the internet does not ensure anonymity from Internet Service Providers (ISP's) [18].

In terms of Dark Web and Dark Web Marketplaces, The Onion Router (TOR) is a popular tool that enables anonymity from ISP's while browsing on the Dark Web [17]. Cryptocurrencies are also a critical technology that allows anonymity on Dark Web Marketplaces. Cryptocurrencies such as Bitcoin provide strong anonymity to their users and

DOI 10.18293/DMSVIVA2023-017

transactions. Thus, it became a vital technology in opening the first Dark Web marketplace; Silk Road [11].

A. The Onion Router (TOR)

The very foundation of the Dark Web and its activities, such as its marketplaces, are based on Onion Routing. The TOR project was created and launched by the US Navy in 2002 to warrant networked anonymous communication [22]. Initially, TOR was created to avoid political censorship and enable freedom of speech over the internet but has since been adapted to facilitate various other activities, including illegal activities [23]. TOR was designed as a low-latency network, a network developed to handle a high capacity of data messages with very little delay or latency while performing functions such as web browsing [24]. The anonymity aspect is achieved through the concept of onion routing. Onion routing allows users to redirect their internet traffic through other users' devices such that the identity of the original user cannot be differentiated from the various other users [25].

Since an essential factor behind anonymity with TOR is to mask one's identity in a sea of various other identities, the soundness of one's anonymity on TOR depends on the number of users on the system [24]. It also depends on whether users on the TOR system are undetectable. If a particular user becomes de-anonymized on the TOR network, this decreases the anonymity level for other users putting the entire network at risk (25). Thus, a knowledgeable understanding of how to download, install and correctly use the TOR software is crucial in ensuring TOR's anonymous integrity [24]. With the demand for online anonymity increasing, TOR has improved its ease of use and provided a mobile version of the software [26]. The Inevitability theory of technology states that once a technology is created, what comes after is its inevitable development [28]. Therefore, TOR's development and advancements will only continue and, if not regulated correctly, could pose challenges for law enforcement.

B. Cryptocurrencies

Cryptocurrencies are a form of digital money that enables users to conduct peer-to-peer (P2P) transactions without the need for centralization [29]. Since cryptocurrencies are a decentralized technology, government and banking institutes have no control. Furthermore, cryptography and blockchain technologies ensure the privacy and security of users and their transactional information [30]. One of the first cryptocurrencies created was Bitcoin in 2009 [7]. As Bitcoin provides a level of security to its users and transactions, and as the cryptocurrency is a decentralized technology, it became a crucial technology in opening the first dark web marketplace, Silk Road. Silk Road's users purchased various illegal items from the marketplace, with payment being made in Bitcoin [11]. Following the fall of Silk Road, various other marketplaces began to rise, and all made use of cryptocurrencies to facilitate their transactions [11]. Since the establishment of cryptocurrencies, there has been a spike in cybercrime worldwide. Having these Dark Web Marketplaces hosted on TOR and facilitated by Bitcoin transactions made it almost impossible for law enforcement and government to regulate illegal activity on marketplaces [30]. A challenging aspect for government and law enforcement regarding cryptocurrencies is that they are decentralized. Meaning no central entity controls it, making it difficult to establish a regulatory framework [32].

C. Decentralization

Most software applications developed adhere to the centralized client-server model by where a central system controls the application. Few applications follow a distributed approach, but very few software applications are decentralized [33]. Decentralized applications can function in two ways, either run on blockchain technology (which is based on peer-to-peer communication) or in a peer-to-peer (P2P) network itself. A significant drawback to Dark Web marketplaces is that they are a centralized entity, meaning a central figure (marketplace admin) controls marketplace activity. A decentralized version of these marketplaces would mean cutting out the middleman and having buyers and sellers interact directly with one another [34].

D. Law Enforcement and Government Intervention

This literature review has highlighted the various technical factors that make the Dark Web and its marketplaces challenging to govern and regulate. Factors such as blockchains and cryptocurrencies decentralized nature where no central entity controls them [32]. Or how TOR's anonymity and encryption attribute inhibit law enforcement in locating cybercriminals [38]. [40] proposes two solutions in decreasing Dark Web-related crime. Solution 1 would be to block access to TOR. Although this will significantly reduce Dark Web-related crime, it would be unfeasible as TOR has a wide range of use cases. The second solution would be to target hidden services. This solution does not have severe repercussions as the first, but it would be more challenging to implement [40].

E. Conceptual Model and Hypotheses

Fig. 1 below presents a conceptual model, of the technological factors influencing the nature of dark marketplaces.

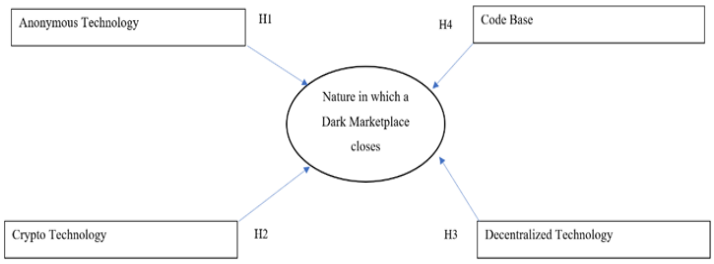

Fig 1. Conceptual model for the study.

The study hypothesises the following:

H1: The type of anonymizing software used to access a dark web marketplace site will influence or determine the nature in which that dark marketplace becomes out of service.

H2: The cryptocurrency used to purchase illegal goods and services from a dark web marketplace will influence or

determine the nature in which that dark marketplace becomes out of service.

H3: There is an association between marketplaces supporting decentralization and the nature in which the marketplace becomes out of service.

H4: The software in which dark web marketplaces are developed will influence or determine the nature in which that dark marketplace becomes out of service.

III. METHODOLOGY

The researchers adopted an objectivism ontological stance and positivism epistemology to guide this study [44], [45]. The study was cross-sectional, and data was collected via a secondary quantitative research method. Collecting large data sets over an extended period of time pertaining to Dark Webs and Dark Web Marketplaces is unfeasible due to time constraints [46]. According to [47], conducting Dark Web data collection requires the researcher to have extensive technical knowledge with web scraping, crawling tools, and routing software. [47] also states that if collecting Dark Web data in such a manner is not feasible, researchers can draw information from digital archives. Material that could be utilized to study Dark Web architecture includes Dark Web forums, mailing lists, hidden sites, and software repositories [47]. Hence classifying the secondary data as multiple-source secondary data as data can be collected from both survey and documentary secondary data [46].

A. Sampling

Obtaining data related to an entire population or all the Dark Web marketplaces functioning on the Dark Web is impractical [42]. The impracticality is derived from the difficulty of identifying all marketplaces on the Dark Web due to the technologies used to keep sites hidden [5]. In such cases, a sampling technique would allow the researcher to only source data on a subset of an entire population or subset of all existing Dark Web marketplaces [50].

As this research deals with the Dark Web and secondary data collection, purpose sampling was adopted [51]. Obtaining data related to the Dark Web can be challenging with all the technical expertise required for collection procedures such as web scraping and crawling, making a purpose sampling strategy suitable. The drawbacks, however, of such a sampling strategy is that it becomes difficult to create a generalization for a population based off the subset chosen.

B. Data Collection

Secondary data was collected from Darknet Market Archives (DNM), an online dark web repository containing Information regarding Dark Web Marketplaces [48]. The DNM archive has been publicly released, and information relating to 87 Darknet Marketplaces was collected [48]. Data relating to the marketplace's technological capabilities, such as the anonymizing software being utilized, the types of cryptocurrencies used to finance transactions being utilized, the codebase in which the marketplace was developed, and whether marketplaces started implementing decentralized technologies were collected. In addition to this, data relating to law enforcement and government efforts were also collected from the DNM, such as the reasoning behind marketplace closing and the success rate of a law enforcement raids.

The data were thus placed into six categorical variables: anonymization, cryptocurrency, decentralisation, codebase, reasoning for marketplace closure, and law enforcement success rate, similar to the original DNM Archive [48]. Each category relates to a section discussed in the literature review chapter of this study where both reasoning for marketplace closure and law enforcement success rate refers to *Law enforcement and Government Intervention.*

To ensure the quality and suitability of the data for analysis, the researchers took several measures to mitigate the potential risk of using inconsistent data. First, reliability and validity tests to evaluate the data's quality and consistency were conducted. While the data size may be limited due to the exploratory nature of the study, the reliability and validity tests suggested fair reliability, indicating that the data could be used for analysis. However, the researchers acknowledged that the data collected from web scrapes and crawls can be prone to external factors such as internet connectivity issues and bugs in the crawling software. Therefore, they took additional steps to verify the accuracy of the data by cross-referencing it with other sources where possible. Overall, these measures helped to ensure the quality and reliability of the data, reducing the risk of confounding the study results. [49].

C. Ethical Considerations

The researchers obtained for ethics approval from the university of Cape Town. Internet-mediated research uses the internet or computing device to conduct archival research and collect secondary data. Secondary data collected and published in a public setting, such as an online data repository, does not require extensive ethical considerations [53]. However according to [46], the sources from which the data was collected should also be distinctly acknowledged, and, if provided, citation guidelines offered by the online repositories should be adhered to.

D. Assessing Reliability and Validity

To assess the reliability and validity of the secondary data collected, it was recommended by [54] to identify copyright statements and published papers utilizing the data. The data set released by [48] was released under the Creative Commons CC0 "No Rights Reserved" license. The Creative Commons (CC) license is a copyright license that defines how information can be distributed. It is utilized in cases where the owner of a piece of work wants to give free access to their work with the intention for their work to be built upon by other users [55]. [54] proclaims that obtaining the data source's copyright statement indicates who is accountable for the data. By obtaining the publications in which the dataset is being utilized, according to [54], will assert the data's reliability as publications are deemed further reliable.

E. Data Analysis

Data analysis was performed using IBM Statistical Package for the Social Sciences (SPSS). A descriptive analysis was first

performed to give a basic description of the data collected. This involved describing each variable's distribution, its central tendency, and the relationship between variables. This analysis is presented in the form of a frequency distribution table, bar charts, and cross-tabulation tables [59]. Following this, regression analysis and hypotheses testing were performed. This allowed for the hypotheses presented in chapter two to be tested by performing a Fisher-Freeman-Halton Exact Test. And for the research question to be answered by performing a linear regression analysis.

IV. RESULTS

A. Descriptive Analysis

Table 1 below presents the characteristics of the data collected from the DNM. Information on 87 Dark Web Marketplaces was collected. The majority of the marketplaces assessed implemented only TOR as their primary anonymizing software (94.3%), with only a small portion of marketplaces utilizing I2P with or instead of TOR (5.7%) as a means of ensuring anonymity on the Dark Web. Bitcoin was the most popular cryptocurrency used to finance transactions, with 89.7% of marketplaces accepting bitcoin as payment for goods and services. Some marketplaces did offer other forms of payment, such as Litecoin (3.4%) and alternative coins, referred to as 'other' (2.3%). However, a select group of marketplaces offered more than one form of payment, allowing their users the option of either paying in Bitcoin or Litecoin (4.6%). More than half of the marketplaces identified did not offer support for multi signatures (80.5%). The codebase in which marketplaces were developed in was unknown for some marketplaces (29.7%). Other marketplaces did make use of open-source PHP frameworks such as Bitwasp (16.1%) and Nette (2.3%) to develop their site. However, a significant portion of marketplaces did decide to custom build their marketplace site (31%). In terms of the reasoning as to why Dark Web Marketplaces stopped operating, 40.2% seized its operations due to scams conducted by marketplace operators, 16.1% were because of hacks that forced closure, 6.9% of marketplaces closed for unknown reasons, and 26.4% were voluntary closures by marketplace operators. From all the 87 marketplaces assessed, only 10.3% were brought to closure by law enforcement. And an even smaller percentage (8%) resulted in the prosecution of marketplace operators.

TABLE I. Frequency distribution describing data collected

Anonymization	**Frequency**	**Percentage**
TOR	82	94.3
I2P with or instead of TOR	5	5.7
Cryptocurrency	**Frequency**	**Percentage**
Bitcoin	78	89.7
Litecoin	3	3.4
Both Bitcoin and Litecoin	4	4.6
Other	2	2.3
Decentralization	**Frequency**	**Percentage**
Made use of Multi signatures	17	19.5
Did not make use of Multi signatures	70	80.5
Codebase	**Frequency**	**Percentage**
Custom	27	31
Bitwasp	14	16.1
Nette	2	2.3
Other	19	21.8
Unknown	25	29.7
Reasoning for Marketplace Closure	**Frequency**	**Percentage**
Law enforcement Raid	9	10.3
Hacked	14	16.1
Scam	35	40.2
Voluntary	23	26.4
Unknown	6	6.9
Law Enforcement Success Rate	**Frequency**	**Percentage**
Led to prosecution	7	8.0
Did not lead to prosecution	80	92.0

As is the case for descriptive data, to measure the central tendency, which is to identify the most frequent value, the mode, will be most appropriate [59]. Table 2 below presents the mode for each category in the data set. For the anonymization category, TOR was the most frequently used anonymizing tool. Bitcoin was identified as the most popular cryptocurrency to purchase goods and services from marketplaces. Custom-built marketplaces were the most common choice taken by marketplace operators when developing the marketplace site. Scams were the usual way in which marketplaces closed. And finally, out of all the 87 illegal marketplaces, 80 of them did not face any legal repercussions.

TABLE II. The Mode for each categorical variable in the dataset

Category	**Mode (Count out of 87)**
Anonymization	TOR (82)
Cryptocurrency	Bitcoin (78)
Decentralization	Did not make use of multi signatures (70)
Codebase	Custom (27)
Reasoning for Marketplace Closure	Scam (35)
Law Enforcement Success Rate	Did not lead to prosecution (80)

B. Interdependence between Anonymizing Technology and Marketplace Closure Reasoning

A cross-tabulation analysis will be suitable to analyse the interdependence between two variables [46]. Table 3 below

illustrates the interdependence between the anonymizing technology used and the nature in which the marketplace closed. Overall, 10.3% of marketplaces were using some form of anonymizing software and getting raided by law enforcement. However, 11% of marketplaces implementing TOR succumbed to a law enforcement raid which is more than the total amount of marketplaces getting raided (10.3%). An adjusted residual value above 2 indicates that the observed frequency for a particular cell is more than the frequency expected for that cell. An adjusted residual value below -2 suggests that the observed frequency for a specific cell is smaller than the frequency expected for that cell [60]. As the adjusted residual is either below 2 or above -2, there is no deviation explaining that 11% is not statistically differentiable from the total of 10.3%. This interpretation was similar for reasoning consisting of Hacked, Scam, Voluntary and Unknown, where the percentage within Anonymizing Technologies is not statistically differentiable from the total value as the adjusted residual values are either below 2 or above -2.

TABLE III. Anonymizing Technology and Marketplace Closure Reasoning

Reason for Marketplace Closure	Anonymizing Technologies		Total
	TOR	I2P with or instead of TOR	
Raid			
Count (%)	9 (11%)	0 (0.0%)	9(10.3%)
Adjusted Residual	0.8	-0.8	
Hacked			
Count (%)	14 (17.1%)	0 (0.0%)	14(16.1%)
Adjusted Residual	1.0	-1.0	
Scam			
Count (%)	34 (41.5%)	1(20.0%)	35(40.2%)
Adjusted Residual	1.0	-1.0	
Voluntary			
Count (%)	20 (24.4%)	3(60.0%)	23(26.4%)
Adjusted Residual	-1.8	1.8	
Unknown			
Count (%)	5(6.1%)	1(20.0%)	6(6.9%)
Adjusted Residual	-1.2	1.2	
Total			
Count (%)	82(100%)	5(100%)	87(100%)

C. *Interdependence between Crypto Technology and Reasoning for Marketplace closure*

Table 4 below illustrates the interdependence between the crypto technology used to finance transactions and the nature in which the marketplace closed. It is evident that the percentage within Cryptocurrencies for Raid, Hacked, Scam, and Voluntary is not statistically differentiable from the total value as the adjusted residual values are either below 2 or above -2. However, 50% of marketplaces that supported both Bitcoin and Litecoin closed for unknown reasons, more than the total amount of marketplaces closing for unknown reasons (6.9%). As the adjusted value is greater than 2 (3.5), significantly more marketplaces support both Bitcoin and Litecoin than expected if there was no dependency between variables.

TABLE IV. Crypto Technology and Reasoning for Marketplace closure

Reason for Marketplace Closure	Cryptocurrencies				Total
	Bitcoin	Litecoin	Bitcoin and Litecoin	Other	
Raid					
Count (%)	8 (10.3%)	1(33.3%)	0(0.0%)	0(0.05%)	9(10.3%)
Adjusted Residual	-.1	1.3	-.7	-.5	
Hacked					
Count (%)	14(17.9%)	0(0.0%)	0(0.0%)	0(0.0%)	14(16.1%)
Adjusted Residual	1.4	-.8	-.9	-.6	
Scam					
Count (%)	31(39.7%)	1(33.3%)	1(25.0%)	2(100.0%)	35(40.2%)
Adjusted Residual	-.3	-.2	-.6	1.7	
Voluntary					
Count (%)	21(29.5%)	1(33.3%)	1(25.0%)	0(0.0%)	23(26.4%)
Adjusted Residual	.3	.3	-.1	-.9	
Unknown					
Count (%)	4(5.1%)	0(0.0%)	2(50.0%)	0(0.0%)	6(6.9%)
Adjusted Residual	-1.9	-.5	3.5	-.4	
Total					
Count (%)	78(100%)	3(100%)	4(100%)	2(100%)	87(100%)

D. *Interdependence between Decentralized Technology and Reasoning for Marketplace closure*

Table 5 below illustrates the interdependence between marketplaces implementing decentralized technologies by offering support for multi signatures and the nature in which the marketplace closed.

TABLE V. Decentralized Technology and Reasoning for Marketplace closure

Reason for Marketplace Closure	Decentralized Technologies		Total
	Did not support Multiple Signatures	Support Multiple Signatures	
Raid Count (%) Adjusted Residual	6(8.6%) -1.1	3(17.6%) 1.1	9(10.3)
Hacked Count (%) Adjusted Residual	12(17.1%) .5	2(11.8%) -.5	14(16.1%)
Scam Count (%) Adjusted Residual	28(40.0%) -.1	7(41.2%) .1	35(40.2%)
Voluntary Count (%) Adjusted Residual	19(27.1%) .3	4(23.5%) -.3	23(26.4%)
Unknown Count (%) Adjusted Residual	5(7.1%) .2	1(5.9%) -.2	6(6.9%)
Total Count (%) Adjusted Residual	70(100%)	17(100%)	87(100%)

E. Regression Analysis

To perform a regression analysis with categorical input variables, each variable will subsequently be transformed into dummy variables. This involves coding the data as 1's and 0s. Where 1 refers to a data point that belongs to a category and 0 for all data points that do not belong. Thus, treating the categorical input variables as a continuous variable for analysis [61]. Presented in table 6 are the results of the regression analysis performed for each independent variable on the dependant variable, represented as two values r (coefficient of correlation) and r^2 (coefficient of determination). The R-value for each variable ranges between 0 and 0.2, indicating a weak but positive correlation between the variables and a low likelihood for the dependant variable to be influenced by the independent variable. With crypto technology having the most significant influence on the nature in which a Dark Marketplace closes. The r^2 values indicate that 0.7% of the dependant variable is predicted by anonymous technology, 2.8% is predicted by crypto technology, 3.7% is predicted by the codebase in which marketplaces are developed, and 1.4% by decentralized technology.

TABLE VI. Results of regression analysis

Independent Variable	Dependent Variable	
	Nature in which a Dark Marketplace closes	
	r	r^2
Anonymous Technology	0.084	0.007
Crypto Technology	0.166	0.028
Code Base	0.091	0.037
Decentralized Technology	0.118	0.014

F. Hypotheses Testing

A Fischer's Exact Test of Independence was deemed appropriate to test the hypotheses (62). A Fischer's Exact Test of Independence is also recommended for analysis in situations where cross-tabulation tables are of 2x2 matrices, and the sample size of the data set is less than 1000, in this case, 87 (63).

Presented in table 7 are the results of conducting the Fischer's Exact test on each of the hypotheses. A probability value P of less than 0.05 indicates a significant association between the independent and dependant variables (46). Based on the Fischer's Exact test conducted in SPSS and presented in table 7, it is evident that none of the four hypotheses established have a significant association between the independent and dependant variables, indicating that neither of the four hypotheses was supported. H1 (P-value= 0.221), H2 (P-value = 0.277), H3 (P-value = 0.859), and H4 (P-value = 0.828) all have p-values greater than 0.05.

TABLE VII. Results of Hypotheses Testing

Hypotheses	Independent Variable	Dependent Variable	Fisher-Freeman-Halton Exact Test		Supported?
			Value	P-value	
H1	Anonymous Technology	Nature in which Dark Marketplace closes	4.655	0.221	No
H2	Crypto Technology	Nature in which Dark Marketplace closes	11.941	0.277	No
H3	Decentralized Technology	Nature in which Dark Marketplace closes	1.595	0.859	No

H4	Code Base	Nature in which Dark Marketplace closes	11.208	0.828	No

V. DISCUSSION OF FINDINGS

Anonymizing technologies serve as the foundation to the dark web and its marketplaces, with TOR being the most popular tool identified within literature [17]. TOR's popularity was justified during analysis, with a large majority of the 87 marketplaces sampled using TOR and only a select few marketplaces implementing I2P. This can be attributed to the reliable anonymity that TOR provides and its constant improvement, with developments made to its ease of use and enabling mobile access to the software [26]. Marketplaces closing because of scams were most prevalent for TOR, whereas marketplaces utilizing I2P were mostly voluntary closures from the marketplaces sampled. However, H1 results show that there was no significant evidence in determining whether the type of anonymizing technology being used within a marketplace will influence the way in which that marketplace closes. Thus, as [32] and [64] discussed, establishing an overarching regulatory framework will be appropriate as this can target the use cases of such technologies. Summarily for crypto technology, with Bitcoin being the most popular among marketplaces in financing anonymous transactions and some marketplaces also incorporating Litecoin to mitigate the slow clearance rate of transactions. Yet, according to the results of H2, there was no significant association between the type of cryptocurrency utilized and the nature in which the marketplace closed. Again, this illustrates that instead of regulating a specific cryptocurrency, policies relating to digital currencies and their use cases should be developed [32].

Dark web marketplaces are vulnerable to closures due to their centralized nature, with a central entity managing the marketplace [65]. Decentralized applications, on the other hand, are more resistant to closures. OpenBazaar, for example, uses multi signatures to enable decentralization, but most other marketplaces analyzed do not support multi signatures. This is because many marketplaces follow a centralized client-server model. This was consistent in literature as many applications adhere to a centralized client-server model [33]. Hence, there was no association between marketplaces supporting decentralization and the nature in which the marketplace had closed thus supporting the results of H3.

The software used in the development of marketplace can mitigate the risk of closures. Java-based codebases are a good solution, as they allow marketplaces to migrate from server to server as many marketplaces analyzed adhered to a centralized client-server model [66]. However, several marketplaces use PHP Frameworks such as Nette and Bitwasp. While Bitwasp supports multi signatures and allows marketplaces developed with the framework to function independently of central servers, H4 results showed that the type of codebase used by marketplaces does not necessarily determine their ability to resist closures or support decentralization.

Each technological factor, anonymization, cryptocurrencies, decentralization, and codebase had a low likelihood of influencing how a marketplace seized its operations, with crypto technology having the greatest significance out of the four technologies identified. This is not unexpected as cryptocurrencies provide both strong anonymity and the ability to enable the sale of illegal goods on the dark web.

VI. CONCLUSION

The study conducted aimed at understanding how dark web marketplaces operate, especially in terms of the various technologies and their impacts on marketplace closures. It was identified in the literature that anonymization provided with software such as TOR and cryptocurrencies like Bitcoin are fundamental components in enabling marketplace activity. This was echoed in the findings of this study as both TOR and Bitcoin were extensively applied throughout marketplaces. The codebases and decentralization were then characterized as additional techniques to mitigate against shortcomings such as the single point of failure with centralized applications. However, the findings of the study confirmed that despite centralization being such a pitfall for marketplaces, most marketplaces still opted not to implement multi signatures or develop marketplaces with codebases that supported it. The technological factors linked to dark web marketplaces closures all had a low probability of determining how a marketplace would become out of service. However, crypto technology was found to have the most impact in allowing dark web marketplaces to operate, thus, illustrating the importance of effective regulation of crypto technology, focusing on its use cases to reduce illegal online activity.

VII. LIMITATIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

The secondary data collected to conduct this research study was bounded by the period in which the data was initially collected. According to the Darknet Market Archives (DNM) dataset, its last known update date was June the 9th, 2019. Many archival datasets relating to the dark web are not updated regularly because of the difficulty and cost of web scraping and crawling dark websites. And the potential for newer techniques or technologies to be implemented within marketplaces has not been accounted for. As technological advancements are rapidly increasing, future research should consider the timeframe in which data collection took place. If possible, primary data should be collected and made available to the public to extend the research opportunities to fields that do not possess the required technical expertise to collect the data.

REFERENCES

[1] D. S. Rudesill, J. Caverlee, and D. Sui, "The deep web and the Darknet: A look inside the internet's massive black box," Woodrow Wilson International Center for Scholars, STIP, vol. 3, pp. 1-17, October 2015.

[2] D. Kolb, "Surface Web is Only the Tip of the Iceberg," Traversals, Available: https://traversals.com/blog/surface-web/. [Accessed: June. 23, 2022].

[3] J. Frankenfield, "*Deep Web*." Investopedia. Available: https://www.investopedia.com/terms/d/deep-web.asp. [Accessed: December. 24, 2022].

[4] Kaspersky, "What is the Deep and Dark Web?" Available: https://www.kaspersky.com/resource-center/threats/deep-web. [Accessed: December. 14, 2021].

[5] E. Jardine, "The Dark Web dilemma: Tor, anonymity and online policing. Global Commission on Internet Governance Paper Series, No. 21, pp. 1-13, September 2015.

[6] A. Gupta, S. Maynard, and A. Ahmad, "The Dark Web as a Phenomenon: A Review and Research Agenda," in the Proc. 30th Australasian Conference on Information Systems, Perth, Australia, pp. 1-12, December 2019.

[7] C. Dipiero, "Deciphering cryptocurrency: Shining a light on the deep dark web," University of Illinois law review. vol. 3, pp. 1267-1299, March 2017.

[8] S. Sadik, and M. Ahmed, "An overview of the Dark Web," in *Security Analytics for the Internet of Everything,*, M. Ahmed, U. Barkat, and A. Pathan, Eds. New York: CRC Press, 2020, pp. 55-66.

[9] Z. Mador, "Keep the dark web close and your cyber security tighter," Comput. Fraud Secur, no. 1, pp. 6–8, January 2021

[10] K. Soska, A. Kwon, A. Christin, N. Devadas, and S. Beaver, "A decentralized anonymous marketplace with secure reputation," Technical Report 2016/464, IACR Cryptology ePrint Archive, pp. 1-15, 2016.

[11] D. Stroukal, and B. Nedvedová, "Bitcoin and other cryptocurrency as an instrument of crime in cyberspace," Proc. of 4th Business and Management Conferences, Istanbul, vol. 4407036, pp. 219-226, October 2016.

[12] S. He, Y. He, and M. Li, "Classification of Illegal Activities on the Dark Web," Proceedings of the 2019 2nd International Conference on Information Science and Systems, Taiyuan, China, pp. 73-78, March 2019.

[13] I. Ladegaard, "Open Secrecy: How Police Crackdowns and Creative Problem-Solving Brought Illegal Markets out of the Shadows," Soc Forces, vol. 99, pp 532-559, November 2020.

[14] Dnstats.net. "List of Darknet Markets in 2021." Available: https://dnstats.net/list-of-darknet-markets/[Accessed: December. 24, 2022].

[15] N. House, "The 2021 Guide to Darknet Markets. The Cyber Security Company. Available: https://www.stationx.net/the-2021-guide-to-darknet-markets/, Jan. 14, 2022 [Accessed: December 15, 2022]

[16] E. Jardine, "Tor, what is it good for? Political repression and the use of online anonymity-granting technologies," New media Soc, vol. 20, pp. 435-452, February 2018.

[17] S. Winkler, and S. Zeadally, "An analysis of tools for online anonymity," Int. J. Pervasive Comput. Commun., vol. 11, pp. 436-453, November 2015.

[18] R. Kang, S. Brown, and S. Kiesler, "Why do people seek anonymity on the internet?," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Paris, France, pp. 2657-2666, April 2013.

[19] S. Larsson, M. Svensson, M. de Kaminski, K. Rönkkö, and J. Alkan Olsson, "Law, norms, piracy and online anonymity," J. Interact. Mark., vol. 6, pp. 260–280, October 2012.

[20] H. Arora, "Possible Silver Lining for the Content-Owners in Illegal File-Sharing Acts," Available at SSRN 3614389, May 2020.

[21] A. D. Berkowitz, "Applications of social norms theory to other health and social justice issues," in The social norms approach to preventing school and college age substance abuse: A handbook for educators, counselors, and clinicians, H. W. Perkins, Ed. Jossey-Bass:Wiley, 2003, pp. 259–279.

[22] A. S. Beshiri and A. Susuri, "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review," JCMC, vol. 07, pp. 30–43, 2019.

[23] A. Chaabane, P. Manils, and M. A. Kaafar, "Digging into anonymous traffic: A deep analysis of the tor anonymizing network," in Proceedings of the 2010 4th International Conference on Network and System Security. IEEE Computer Society, Washington, DC.

[24] K. Gallagher, S. Patil, and N. Memon, "New me: Understanding expert and non-expert perceptions and usage of the Tor anonymity network.," 13th Symposium on Usable Privacy and Security, Santa Clara, California, SOUPS 2017,

[25] J. Clark, P. C. Van Oorschot, and C. Adams, "Usability of anonymous web browsing: an examination of tor interfaces and deployability," Conference Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania, USA SOUPS 2007.

[26] A. Nastuła, "Dilemmas related to the functioning and growth of Darknet and the Onion Router network.," Journal of Scientific Papers "Social development and Security," vol. 10, pp. 3–10, April 2020.

[27] G. N. Nedeltcheva, E. Vila, and M. Marinova, "The Onion Router: Is the Onion Network Suitable for Cloud Technologies'" in Smart Technologies and Innovation for a Sustainable Future: Advances in Science, Technology & Innovation, A. Al-Masri and K. Curran, Eds. Springer: Cham., 2019.

[28] M. Cuneta "Bitcoin's Inevitability Thesis, Understanding the unstoppable nature of technology". Available: https://medium.com/@MiguelCuneta_21450/bitcoins-inevitability-thesis-d89585e62356, April, 2019, [Accessed: June 14, 2021].

[29] S. Lee, C.Yoon, H. Kang, Y. Kim, Y. Kim, D. Han, S. Son, and S. Shin, "Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web," Proceedings of 2019 Network and Distributed System Security Symposium, 24-27 San Diego, CA, USA, February 2019.

[30] M. Milutinović, "Ekonomika," Journal for Economic Theory and Practice and Social Issues, vol. 64, pp 105-122, 2018.

[31] A. Barysevich, & A. Solad, "Litecoin emerges as the next dominant dark web currency. Recorded Future." Available: https://www.recordedfuture.com/dark-web-currency/, March 8, 2018, [Accessed: November 12, 2022].

[32] H. Nabilou, "How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency," Int. J. Law Inf. Technol., vol. 27, pp. 266–291, 2019.

[33] S. Raval, "Decentralized applications: harnessing Bitcoin's blockchain technology." O'Reilly Media, Inc. 2016.

[34] Hussey, M, 'What are decentralized marketplaces?" Available: https://decrypt.co/resources/what-are-decentralized-marketplaces, March, 2020, [Accessed: December 15, 2022]

[35] A. Greenberg, "Inside the 'DarkMarket' Prototype, a Silk Road the FBI Can Never Seize." Wired. Available: https://www.wired.com/2014/04/darkmarket/, April 24, 2014, [Accessed: December 10, 2022].

[36] I. Allison, "Mover over eBay: Countdown to OpenBazaar and the decentralised marketplace revolution." International Business Times. Available: https://www.ibtimes.co.uk/move-over-ebay-countdown-openbazaar-decentralised-marketplace-revolution-1529767, November 20, 2015, [Accessed: December 24, 2022].

[37] J. Redman, "Meet Beaver: A Decentralized Anonymous Marketplace." Bitcoin News, Available: https://www.livebitcoinnews.com/meet-beaver-a-decentralized-

anonymous-marketplace/, May 19, 2016, [Accessed: December 18, 2022].
[38] R. Heaton, "How does Tor work?" Available: https://robertheaton.com/2019/04/06/how-does-tor-work/, April 6, 2019, [Accessed: December 18, 2022].
[39] A. Ghappour, "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web," Stanford Law Review, vol. 69, April 2017.
[40] N. V. Denic, "Government Activities to Detect, Deter and Disrupt Threats Enumerating from the Dark Web," Technical Report, US Army Command and General Staff College Fort Leavenworth United States, 2017.
[41] J. Dalins, C. Wilson, and M. Carman, "Criminal motivation on the dark web: A categorisation model for law enforcement," Digit Investig, vol. 24, pp. 62–71, March 2018.
[42] R. V. Clarke, "Situational Crime Prevention," Crime and Justice, vol. 19, pp. 91–150, January 1995.
[43] K. Hegadekatti, "Regulating the Deep Web Through Controlled BlockChains and Crypto-Currency Networks," SSRN Electronic Journal, pp. 1-10, December 2016.
[44] A. Ahmed, "Ontological, Epistemological and Methodological Assumptions: Qualitative versus Quantitative," Online Submission, pp. 1-13, 2008.
[45] H. Collins, "Creative research: the theory and practice of research for the creative industries," Bloomsbury Publishing: New York, pp. 1-203, 2018.
[46] M. Saunders, P. Lewis, and A. Thornhill, Research *Methods* for *Business Students*. Pearson: New York, 2012.
[47] R. W. Gehl, "Archives for the Dark Web: A Field Guide for Study," in Research Methods for the Digital Humanities, L. Levenberg, T. Neilson and D. Rheams, Eds. Springer Nature: Switzerland AG, 2018, pp. 31–51.
[48] G. Branwen, N. Christin, D. Decary-Hetu, Munksgaard R. Andersen, E. Presidente, Anonymous, Lau, D., Sohhlz, Kratunov, D., Cakic, V., A. Buskirk, Whom, M. Mckenna, & Goode, "Dark Net Market archives, 2011-2015." Available: https://www.gwern.net/DNM-archives S., March 20, 2021, [Accessed: November 20, 2022].
[49] M. P. Johnston, "Secondary data analysis: A method of which the time has come." Qualitative and quantitative methods in libraries, vol. 3, pp. 619-626, September 2014.
[50] M. Saunders, P. Lewis, and A. Thornhill. "Research *Methods* for *Business Students*. Pearson: New York, 2009.
[51] I. Etikan, "Sampling and Sampling Methods," BBIJ, vol. 5, pp. 210-213, May 2017.
[52] A. S. Acharya, A. Prakash, P. Saxena, and A. Nigam, "Sampling: why and how of it?," Indian Journal of Medical Specialities, vol. 4, pp 330-333, July 2013.
[53] L. Cilliers, and K. Viljoen, "A framework of ethical issues to consider when conducting internet-based research," SAJIM, vol. 23, pp. 1-9, March 2021.
[54] N. Ó. Dochartaigh, "Internet Research Skills (3rd ed.)," SAGE Publications, Inc., 2012.
[55] G. Hagedorn et al., "Creative Commons licenses and the non-commercial condition: Implications for the re-use of biodiversity information," ZooKeys, vol. 150, pp. 127–149, November 2011.
[56] K. Kruithof, J. Aldridge, D. Hétu, M. Sim, E. Dujso, and S. Hoorens, "Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands," Rand Corporation: Cambridge, UK, 2016.
[57] S. Ghosh, A. Das, P. Porras, V. Yegneswaran, and A. Gehani, "Automated categorization of onion sites for analyzing the darkweb ecosystem," Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Halifax, NS: Canada 2017.
[58] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The Ransomware-as-a-Service economy within the darknet," Computers & Security, vol. 92, p. 101762, May 2020.
[59] M. K. William, "Research Methods Knowledge Base: Descriptive statistics." Available: https://conjointly.com/kb/descriptive-statistics/, 2021, [Accessed: November 12, 2022].
[60] A. Agresti, "Categorical Data Analysis," Wiley Series in Probability and Statistics, New York: Wiley, 2002.
[61] H. Schielzeth, "Simple means to improve the interpretability of regression coefficients," Methods Ecol. Evol., vol.1, pp. 103–113, February 2010
[62] G. M. Gaddis, and M. L. Gaddis, "Introduction to biostatistics: Part 5, statistical inference techniques for hypothesis testing with nonparametric data," Ann Emerg Med, vol. 19, pp. 1054–1059, September 1990.
[63] L. M. Connelly, "Fisher's exact test," Medsurg Nursing, vol. 25, pp. 58-60, 2016.
[64] A. Spithoven, "Theory and Reality of Cryptocurrency Governance," J. Econ. Issues, vol. 53, pp. 385–393, April 2019.
[65] L. Brittney, "Deep Dot Web Seized. Terbium Labs." Available: https://terbiumlabs.com/2019/07/11/the-king-is-dead-long-live-decentralized-markets/ 2019, [Accessed: November 12, 2022].
[66] M. Shoaib, A. Ishaq, M. Awais, S. Talib, G. Mustafa, and A. Ahmed, "Software Migration Frameworks for Software System Solutions: A Systematic Literature Review," International Journal of Advanced Computer Science and Applications, vol. 8, pp. 192-204, 2017.

".