Darknet markets

competitive strategies in the underground of illicit goods

Evangelista, A.

Award date:
2018

Technische Universiteit Eindhoven University of Technology

Department of Mathematics and Computer Science
Security group (SEC)

Darknet Markets: Competitive Strategies in the Underground of Illicit Goods

Master Thesis

Student:
Andrea Evangelista

Supervisors:
dr. L. Allodi, dr. M. Cremonini

Eindhoven, 10 September 2018

Abstract

Buying and selling drugs on the Internet is gaining more and more momentum, given the advances in anonymizing web technologies which are exploited for illegal goods trading on the so called darknet markets. Those are web platforms where any different kind of illegal goods and services (drugs, weapons, passports, malware) can be traded with ease. Drugs are estimated to account for around two thirds of darknet market activity. Behind the online drug trafficking there are vendors, whose behavior is crucial for their reputation and trustworthiness, and darknet market platforms that make possible for users to virtually meet and trade, in an relatively safe and anonymous manner. However, given the illicit nature of traded goods and the profit made, law enforcement is constantly active in monitoring, seizing and closing platforms, performing several arrests every year. The goal of markets participants is therefore to minimize the risk of being exposed, scammed or harmed, while increasing the utility derived from buying or selling the merchandise. This thesis presents a systematic analysis of the online underground ecosystems, with a focus on features, strategies and mechanisms which may be exploited by darknet markets to differentiate from the competition, attract more users and generate more profits. We relate core problems of the underground economy to features platform implement to mitigate those issues. We conclude that most profitable and attended markets do not tend to be safer than smaller platforms and do not seem to gain popularity through specific mechanisms that may encourage illicit trading (e.g. safer transaction methods, low risk of scam and arrest, support in case of disputes, loyalty awards, harm reduction). We find that alternative more secure and reliable platforms are emerging, but are still small, with less availability of goods, few users and more concentrated profits.

Acknowledgements

I would like to express my greatest appreciation to the people who have helped and supported me throughout my master project.

To my supervisor at the Technical University of Eindhoven, Dr. Luca Allodi, who provided me with guidance during my research in terms of motivation, valuable feedback and significant new point of views on various topics.

I would also take the opportunity to thank my supervisor from the University of Milano, Marco Cremonini. He provided me with valuable additional thoughts on matters, critical feedback and eye-opening suggestions. Without their passionate participation and input, this project could not have been successfully performed.

Additionally, I would like to thank the whole committee and staff that made it possible for me to conduct my studies and final thesis at the Technical University of Eindhoven.

Last, but not least, I would like to thank my family and friends for providing me with an unfailing support, love, care, understanding and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. Had it not been for them, the outcome of this project would not have been the same.

Finally, I would like to take the opportunity to thank everyone whom directly or indirectly supported me in any way by contributing to my masters thesis.

Gratefully yours,
Andrea Evangelista

Contents

Contents **vii**

List of Figures **ix**

List of Tables **xi**

1 Introduction **1**
- 1.1 Thesis contributions . . . 4
- 1.2 Scope of work . . . 4
- 1.3 Research question . . . 5
- 1.4 Thesis outline . . . 6

2 Background and related work **7**
- 2.1 History and timeline of darknet markets . . . 7
- 2.2 Drug trafficking in the cyber space . . . 8
- 2.3 Core problems of the underground economy . . . 9
  - 2.3.1 Moral hazard and adverse selection . . . 9
  - 2.3.2 Trust and reputation . . . 11
- 2.4 Underground e-marketing techniques . . . 13

3 Methodological approach **15**
- 3.1 Market sampling . . . 15
- 3.2 Qualitative data collection . . . 18
  - 3.2.1 Attribute of interests . . . 18
- 3.3 Quantitative data collection . . . 19
  - 3.3.1 Crawling and scraping Tor onion sites . . . 20
  - 3.3.2 Datasets . . . 21

4 Comparative qualitative analysis of markets **23**
- 4.1 Exploratory analysis of sampled markets . . . 23
- 4.2 Summary of findings . . . 31
  - 4.2.1 Mechanisms addressing moral hazard . . . 32
  - 4.2.2 Mechanisms addressing adverse selection . . . 33
  - 4.2.3 Other mechanisms . . . 34

5 Quantitative evaluation of market setups **37**

6 Discussion and Conclusions **45**

6.1 Limitations 47

Bibliography **49**

List of Figures

1.1 A Dream Market web page 2

2.1 Escrow process 12
2.2 2-out-of-3 multisignature BTC address creation and payment process 13

3.1 Dream Market DoS protection mechanism 19
3.2 Scraping process 20

4.1 Dream Market HTML and JavaScript files 25
4.2 Dream Market IP leak from market.js 25
4.3 Dream Market IP leak from index.html 25
4.4 CGMC homepage 28
4.5 CGMC discussion forum 28

5.1 Distribution of revenues per sale of vendors on each platform 41
5.2 Distribution of vendors based on their join date and average revenue per sale (logarithmic scale) 42
5.3 Distribution of vendors based on their join date and revenues generated (linear scale) 43

List of Tables

3.1 Three of the most popular darknet forums and user communities 16
3.2 Tiers 18
3.3 Sampled markets under study 18
3.4 Scraping information 21
3.5 An excerpt of the dataset 21

4.1 Reverse IP lookup of Dream Market leaked addresses 25
4.2 Markets comparison based on security features 29
4.3 Markets comparison based on payment methods 29
4.4 Markets comparison based on agent selection features 30
4.5 Markets comparison based on and marketing features 31
4.6 Vendor application 31
4.7 Exploratory observations 32

5.1 Statistics of the scraped platforms 38
5.2 Top 20 vendors based on total revenues 40

Chapter 1

Introduction

In the last decade online trading of illegal goods on hidden web sites has witnessed a significant growth. Thanks to recent innovations in digital currencies and anonymous networks, new business models for illicit trading have been encouraged and, as a consequence, appealing and somehow less risky environments for traders have flourished: the so called cryptomarkets or darknet markets (DNMs).

DNMs operate in a hidden part of the web, which is not accessible by standard and usual browsers, and where anonymization services are in place. Using Tor (The Onion Router) network through the Tor web browser is a first step to hide one's own IP address when accessing a website. Anonymous or untraceable cryptocurrencies are used to make safe payments of illegal goods. Encrypted communication between market participants is strongly encouraged and to some extent enforced by DNMs developers. On those platforms different kind of illegal goods and services (e.g. drugs, weapons, passports, malware) can be traded with ease, generating revenues for vendors, profits for platform owners, satisfaction for buyers and, in general, utility to markets participants. DNMs are structured as e-commerce platforms (along the lines of Amazon or eBay marketplaces) which facilitate the exchange of goods and money among users (buyers and vendors) and possibly generate profit through commission fees over purchases. In Figure 1.1 a web page of Dream Market, one of the most popular DNMs, is shown. The layout is quite simple and the interaction with the website is intuitive. After a straightforward registration process (similar to any other website and where no email address is needed), which mainly involves the choice of username and password, it is possible to access the platform and start trading. Registered users can browse the listings of goods which are sold, visit any section of the website and adjust their profile settings according to their preferences (e.g. login method and preferred currency). Moreover searching products and filtering results are basic standard features implemented by any platform.

Generally, platforms role is to act as intermediaries between vendors and buyers, for instance by making it easier for the former to advertise their products and for the latter to search and compare products prices, reviews and descriptions. In addition platforms play the role of trusted third parties in case of disputes or complaints, being able to refund defrauded users or ban a vendor accused of selling prohibited goods or proven to be scamming his/her customers. Moreover by using digital platforms, users can buy illicit products without incurring in the risky street dealing activity [23, 40, 22]. On the other hand vendors may be able to remain hidden and at

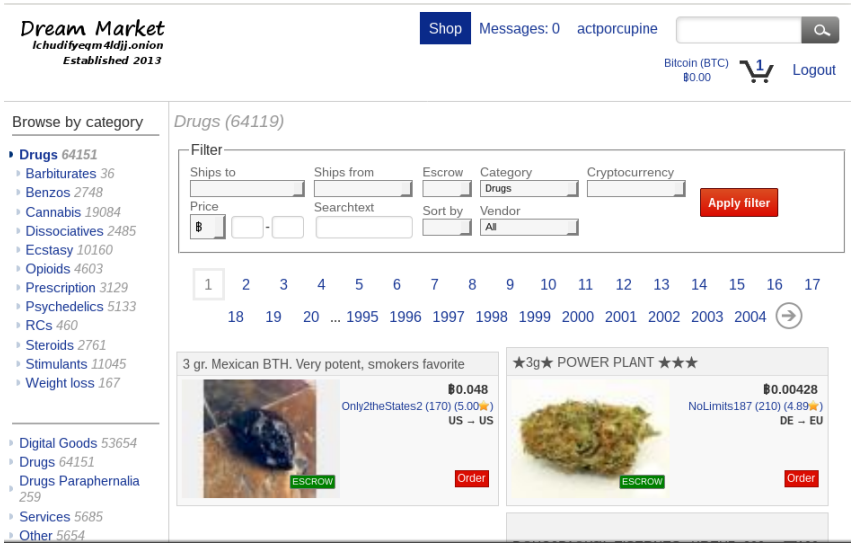

Figure 1.1: A Dream Market web page

the same time receive large payments of purchases through cryptocurrencies, which can be more difficult to trace back to the source. Finally markets owners make profit through commission fees on purchases: the larger the number of users and trades on their website, the higher the profit. Therefore platforms have to be appealing for potential users. Being criminal markets, it is critical to assure a safe environment in terms of personal data security and privacy, correct and anonymous transactions, absence of scammers and quality of goods.

The presence of actors in the market (and the consequent market longevity) is driven by "classic" economic and behavioral choices, which range from the reduced risk of street violence to the utility cost of a particular sale, till the absence of credible alternatives. Motivations and (implicit) decision factors may lead to the choice of a market rather than another, with different concerns and motivations among buyers and vendors.

Users motivations

Usually users join a darknet community and register themselves to a DNM for different reasons. Curiosity, research and the one for which the first two exist: illicit trading activities [16]. It is plausible to think that DNMs users (potential buyers and vendors) want to feel (and actually be) safe while browsing the DNM website, never engage with scammers and lose money. Moreover they do not want to engage with Law Enforcement (LE) agents in any manner. Buyers seems to be motivated to buy drugs online due to a perception of better safety, reviewed quality and product variety, anonymity and home delivery [35]. The risk of not being able to satisfy any or some of the above requirements may be assessed in different ways by different customers and the feeling of safety and security may be subject to change over the time. This is due to the likely variety of type of customers, ranging from expert users to newbies hardly using any security measure and prone to being scammed. On the other hand, expert buyers and vendors are more likely to be subject of interest of law enforcement investigations. Similarly, market players who purchase or sell large quantities of illicit goods may have different identities for different purchases. To be

noted, however, that vendors might be reluctant to start trading with unknown buyers for which they do not have any information.

Hence, buyers' concerns are security of platform, price and quality of goods and support in case of fraud and disputes. Vendors, instead, are likely more interested in market size and volume, competition and room for profits; in addition security of platform and buyers verification play an important role. Finally both buyers and vendors are concerned about the risk of being exposed to law enforcement investigations. In fact it is well known among darknet markets users that some platforms are monitored by authorities and some might be also run by law enforcement, as in the case of Hansa Market run by Dutch police for a little while [9].

Market success

Although trading in illegal markets might sound as a risky and unsafe activity, evidence shows that significant revenues are made and ordered goods correctly reach their destinations [30], as well as there are continuously reported arrests, packages interceptions and seizures [11, 8, 13]. Moreover in the light of the fact that drug trade on DNMs, as a whole, seems to be resilient to law enforcement interventions [25], as new markets quickly emerge and gain share, few questions arise. *How do online illicit markets actors trust each other? How are buyers informed about product quality? How do vendors know they are not shipping to police? Why is it all not only a huge scam? How can criminals trading activity guarantee markets longevity and reliability?*

In order to correctly assess those questions it is important to underline that online illicit goods markets need to adopt regulating mechanisms, to assure a certain level of trust among anonymous criminal agents. The concept of trust can be traced back to two main economics concepts, namely: moral hazard and adverse selection. Moral hazard refers to the problem of behaving in a more risky way than usual, since another party is going to bear the cost of those actions. Hence an agent may decide to act in a risky way in order to gain higher benefits, given that the risk taken will not produce significant losses for her/him. In illegal darknet marketplaces this may lead to irrational behavior based. For instance, some vendors may decide to randomly scam some new inexperienced buyers, because they believe that their overall reputation will not be affected on the long-term. Or, similarly, vendors may just build trust with quality sales for a certain period of time and eventually receive all the following payments without deliver any good or service, until the platform bans him/her. Finally also the platform can misbehave towards its users. For instance, the platform may encourage business and transactions through an escrow service (which users trust and put money in), even knowing that such a system is not safe, since the platform owns the escrow and can eventually steal the coins held. Adverse selection, on the other hand, refers to the ability to assess and recognize goods and agents quality properties in the market. Drugs are a kind of product which is difficult to test before use. Indeed they are considered to be *experience goods* [40], since their quality (in most of the cases) can be tested only after use. Buying drugs online poses the risk of the adverse selection problem, because users have no way of knowing product quality in advance. Therefore buyers lack the information needed to assess the value of a particular product at the moment of purchase. Hence the risk of ordering overpriced low quality item seems to be significant in an environment where anonymity, knowledge asymmetry and lack of governance can seriously affect the decisions made by users.

Darknet markets are becoming more and more sophisticated, thanks to mechanisms, such as

feedback systems, which mitigate some exposure to risk, allowing for an efficient and effective trading among unknown and untrusted parties. Illicit online markets seem also to be aware of the importance of marketing techniques to improve their sales and revenues. Strategies are used and marketing experts hired in order to handle a robust business, thus showing the maturity of illegal darknet markets. As resources in the underground (as in all markets) are limited, competition is a key factor that drives market success. By competing, the underground markets attract the best/more reputable vendors, high-profit goods, and the number of buyers that, ultimately, make up for the mass of the underground economy.

1.1 Thesis contributions

In this work we investigate which mechanisms darknet markets adopt to differentiate themselves from the competition, arguably with the ultimate goal of either attracting specific type of players, or providing an attractive platform that can gather the key players of the economy. Those mechanisms and features should face the core problems of the underground economy, represented by moral hazard and adverse selection. The analysis implemented in this project utilizes qualitative and quantitative methods over data collected and scraped from a chosen set of darknet market platforms, with the intent of formulating insights of the economic and behavioral approach of platform participants.

The focus has been placed upon technical features and marketing techniques adopted by darknet markets, to evaluate whether they constitute key points in decisions and behaviors of vendors, buyers, platform administrators and law enforcement. A particular emphasis has been given to understanding the differences between long-running large platforms (with scarce customer support, lack of anti-scam payment methods, with a wide range of listings) and relatively new website (customer-oriented, with safe payment methods and specialized in few types of goods).

This study considers two aspects of the economics of illicit online drug trading. First, it offers an overview of the main markets operating in the underground, describing features and changes over the time. Second, it looks at whether those features play a role in users strategic positioning and decision making. We propose an exhaustive literature review and offer an up-to-date picture of the illicit underground ecosystem. In addition, we took snapshots of three active darknet market platforms during the last months and wrote scripts which collect, parse and analyze data about vendors, feedback and sales. We conclude that most profitable and attended markets do not tend to be safer than smaller platforms and do not seem to gain popularity through specific mechanisms that may encourage illicit trading (e.g. safer transaction methods, low risk of scam and arrest, support in case of disputes, loyalty awards, harm reduction). However, alternative markets are smaller, with less availability of goods, vendors and more concentrated profits.

1.2 Scope of work

This thesis adopts a strongly multidisciplinary approach by investigating the economic mechanism behind illegal markets operations. Due to the nature of the studied criminal environment, conclusive evidence cannot be gathered (e.g. as direct observation of criminal decisions cannot be

performed). Differently, this work aims at uncovering key economic mechanisms behind darknet markets operations, that can shed light on *how* and *what* measurable platform features could impact decision making. No such study currently exists for online illegal markets. Whereas the adopted approach perhaps stems away from "classic computer science", it allows us to explore an otherwise largely unknown area of criminal operations that directly contributes to the fundamental (as opposed to empirical) aspects of online crime.

1.3 Research question

Given law enforcement seizures, arrests and undercover investigations, it sounds reasonable for markets administrators to prepare their own website to become the next big market, after the large one is taken down. As we have briefly mentioned, the underground ecosystem is populated with darknet markets that may or not play a big role after the closure of a very successful platform. Arguably not all of the owners have the same goals. Owner A and owner B might be interested to enrich their customers base and, thus, may get in competition with each other, while owner C is willing to remain a middle market, since the cost (and benefits) of becoming larger may not worth it (e.g. for niche markets).

It is interesting to investigate whether darknet markets administrators have a wider and forward-thinking view of the context they operate in, or not. Thus, our guiding reasoning focuses on the possible adoption of strategic placement approaches by market administrators with respect to competition among darknet markets. Adoption of particular strategies to face the rapid changes in the overall underground ecosystem and deal with the core problems of moral hazard and adverse selection might minimize the uncertainty derived by law enforcement operations and scammers. We argue that the insights derived by this study are useful for policymakers and law enforcement professionals to have a better understanding of the darknet markets environment.

Studying the literature presented in Chapter 2 we found that regulation and reputation mechanisms form the foundation of a robust and reliable DNM. Thanks to those strategies, market users have more information about sellers, buyers and quality of goods. Hence on average the probability of being scammed by vendors or interact with unreliable buyers should decrease when more information is available. As we have discussed, risk and perception of risk can be mitigated through reputation mechanisms, however there is no standard procedure that guarantees a totally safe and secure environment. In principle the most successful platforms should be those that assure the safest environment to its users. However, is this true? Is there evidence from which we can infer that the most popular and durable DNMs on the scene are also the safest one? Is there any evidence that show an interest into strategic placement by market administrators with respect to competition among darknet markets? Following the this idea of competitive placement among DNMs, we formulate our research question as follows.

Which are the strategies and mechanisms that minimize the uncertainty derived by law enforcement operations and scammers in the market?

In order to address our research question, a mix of quantitative and qualitative methods are applied, consisting of: an extensive literature review; in-depth research through communities,

forums and marketplaces; scraping DNMs to collect and parse data, identify and visualize patterns and to generate valuable insights from the collected evidence.

1.4 Thesis outline

The thesis proceeds as follows. Chapter 2 presents a background on the topic and discusses current relevant literature to set the stage for the discussion of our research. Chapter 3 describes the methodological approach used for our research, focusing on the process of collecting and analyzing data. Chapter 4 presents a comparative qualitative analysis and a summary of findings. Chapter 5 shows the results of a quantitative analysis made on collected data. Chapter 6 presents a discussion of the results of our research, with an emphasis on the limitations and restrictions of our approach. Final thoughts are reported, providing suggestions for future research and conclusions to our thesis.

Chapter 2

Background and related work

In this section a background and a review of the literature on Darknet Markets is presented. The results show that online marketplaces operating in the context of illicit drug trafficking are mature and the behavior of their agents (i.e. the actors involved in the trading, such as buyers, sellers and governance) may be driven by utility, incentives and penalties, such as any other market. Past works focused on the economic analysis of (street) crime demonstrate that the decision to engage in illegal activities is rational [38]. The same seems to apply to the context of illicit underground trading, where well designed and trustworthy marketplaces do exist, in which goods and services are correctly delivered and money transactions happen regularly. While seizures and arrests can shock the underground environment in the short term, the overall ecosystem is resilient and new platform rapidly may become the leading darknet markets in the scene, for number of customers and revenues made. Disruption seems to affect the trades only temporarily. When trusted platforms are taken down, vendors and buyers can switch to other darknet markets which can guarantee more safety and reliability.

2.1 History and timeline of darknet markets

Since 2010 online trading in illicit goods and services has become an interesting business for criminals. The proliferation of data encryption tools and anonymous communication techniques has lead the creation of websites and trading platforms which can assure some sort of privacy and identity protection to their users. One of the first marketplace to exploit the Tor anonymous network [28] for illicit trading was The Farmer's Market, which was shipping narcotics, LSD and cannabis to 35 countries [6]. In 2012 the investigation Operation Adam Bomb, led by DEA, the U.S. Drug Enforcement Agency, together with other international authorities, showed that the marketplace processed around 5,000 orders (worth about 1 million USD) between 2007 and 2009. Buyers used a variety of payment services such as PayPal, Western Union, I-Golder, and Pecunix, and also via cash [5]. In the meanwhile payment technology was witnessing a new revolutionary innovation in the way of exchanging assets trough blockchain and cryptocurrencies, promising and achieving some levels of anonymity and privacy of transactions. In 2009 Satoshi Nakamoto introduced what it is considered to be the first decentralized cryptocurrency: Bitcoin [39]. The idea was to make it possible to perform transactions without the need of a trusted third party,

such as a bank or an intermediary, and in an anonymous manner. By using a network of nodes which relies on cryptography to verify the integrity of data and by using a public distributed ledger (i.e. a database) called blockchain to record transactions, Nakamoto proved the feasibility of such a system in the real world. Indeed as of August 2018 there are 2112 cryptocurrencies in use [1, 18]. Since their first development crypto payments techniques are used in illegal transaction over the internet. The first platform operating on Tor and using Bitcoin for payments was Silk Road, founded by Ross Ulbricht in February 2011 [27]. Silk Road provided an environment for sellers and buyers to conduct transactions using advanced digital encryption and relying on the Tor network to achieve a good level of security, with regard to confidentiality of data and anonymity of transactions.

Key features of Silk Road are the baseline on which every other darknet market is built on. Those are [37]:

- reliance on the TOR network;
- use of traditional postal systems to deliver goods;
- third-party hosting and administration;
- use of encrypted cryptocurrencies (e.g. Bitcoin, Monero).

In October 2013, the Federal Bureau of Investigation (FBI) shut down the website and arrested the founder. Shortly after Urlicht's arrest, on 6 November 2013 Silk Road 2.0 came online, run by former administrators of Silk Road but closed one year later, in 2014, after the Operation "Onymous" [17] took place. However, disruption did not affect the rate at which vendor numbers increased on other markets in the mid-term [25], making the overall ecosystem appearing to be resilient to seizures and closures. In April 2015 Agora was the largest operating market, avoiding Operation Onymous. Just one month before, in March 2015, one of Agoras main competitors, the Evolution market, performed an "exit scam", stealing escrow funds worth 12 million USD. However in August 2015 Agora also closed. Administrators decided to refund sellers and buyers with the money held before shutting down the servers [34]. The following months saw Hansa and AlphaBay as the largest market. However in July 2017 Operation Bayonet took place and culminated in seizures of both Hansa and AlphaBay markets. TradeRoute (which also exit-scammed) and Dream Market were the most popular markets at the time. Dream Market (launched in 2013) is still active and operative. Despite the security leaks and the reported scams, it survived longer than any other market.

At the time of writing there are more than 20 markets that seem to be active. However, the underground community appear to focus on a shorter list of platforms (about 12-14), which seems to be robust, resilient and present an interesting set of features that are discussed in this thesis.

2.2 Drug trafficking in the cyber space

One of the most extensive analysis of darknet markets throughout a significant timespan was made by Soska and Christin in [41]. Over 2 years they documented changes of goods being sold, law enforcement arrests, frauds and revenues, pointing out the increasing adoption of OPSEC measures by vendors (such as encrypted emails). They analyzed the popular Silk Road marketplace, together with other important platforms (Agora and Evolution), and reported how law enforcement arrests and seizures were not actually damaging the overall underground drug trading ecosystem. Their

research focused on the revenues made by vendors on each market, in order to derive a measure of the volume experienced by each platform under study. The result is that darknet markets experience a continuous growth in terms of users and revenues. In addition their findings suggest that markets are resilient to scams and law enforcement take-downs. In fact, aggregate volumes were increasing rapidly short after some significant markets seizures. Moreover their study gave insights about vendors longevity (on average less than a year) and sellers competition (only few vendors generate significant profit).

A recent joint report prepared by the EMCDDA and Europol [30] puts lights on darknet markets function and their relation with criminal behavior. Authors conducted an EU-focused analysis of drug supply on global darknet marketplaces, basing their research on data collected by Soska and Christin [41]. Between 2011 and 2015, revenue and weight analysis of drug sales sees three major countries which stand out: Netherlands, United Kingdom and Germany. The study also describe the diversification of vendors in terms of product offered, showing that about half of all vendors specialize in one category. In particular, among 2180 unique identities, only almost the 18% sells other type of drugs, whereas almost the 54% also sell non-drug products (for example, digital goods).

In [41] authors argue that darknet markets vendors are primarily competing with local street trafficking, rather than large criminal organizations selling huge amount of illegal goods. This is supported also by another recent study of the darknet markets structure has been conducted by Dittus et al.[29]. The authors analyzed the geographic structure of some drug-related markets, showing that for some kind of drugs, darknet markets are not removing or replacing prior supply chains, because trading seems to happen at the "last mile". Darknet markets have the role of local retailers and their existence is driven by the demand. In fact evidence coming from cannabis and cocaine vendors analysis show that sellers are primarily located in a small number of consumer countries. Hence it is plausible to derive a relation between trading and consumption, rather than between trading and production. In other words there is high spatial concentration: a small number of the same countries (US, U.K., Australia, Germany, The Netherlands, Canada and China are responsible for the majority of global trades. In addition for the top trading countries, national consumption of the drug is high, while national production is low [29].

2.3 Core problems of the underground economy

In this section the economic function of illicit online markets is discussed. Information asymmetry problems that arise in these kind of markets are presented, with regard to the concepts of moral hazard and adverse selection. Finally attention is given to the way trust is built among participants in online illegal trading, throughout the means of feedback systems and regulation mechanisms.

2.3.1 Moral hazard and adverse selection

Akin to other markets (e.g. used cars), illicit online trading suffers the problem of information asymmetry, where one of the two parties has better or more knowledge (with respect to the potential trade) than the other. Having different information about, for instance, the quality of a certain product may create significant challenges to a fair and continuous market operation (e.g.

as postulated in Akerlof's seminal work on *lemon markets* [20]). When buyers cannot differentiate between good and bad quality products (called *lemons*), they are only willing to pay a price that is in between the high quality products and the low quality ones. In this scenario of high quality products, sellers either accept to sell at a lower price or decide to exit the market. On the other hand, when quality sellers leave the market, buyers experience a reduced quality in goods and services. Therefore high information asymmetry may eventually lead the market to collapse. An interesting work made by Reuters and Caulkins in [40] investigates the markets of "illegal lemons". Those markets basically show the same characteristics of a "legal lemon" market, although also illicit good vendors have incomplete knowledge about the quality of the goods they sell. For instance it is very unlikely for a street cocaine dealer to know the purity of the substance he/she sells or to have performed any kind of chemical test on it. The reason lays on the distribution chain and supply of illegal goods markets. Their findings show that asymmetry in information generates high price and quality dispersion. Given the difficulties in advertising and testing quality and given the illegal environment, they found the characteristics of markets which lead to price and purity dispersion: unknown quality, high cost of searching the best sale and unpredictable turnover among participants.

DNMs dynamics and behaviors are influenced by the above mentioned characteristics, which constitute the reasons behind information asymmetry in this kind of markets. In those ecosystem, rather than price dispersion, problems as moral hazard and adverse selection are faced. Those affect both buyers, sellers and also the online trading platform. Adverse selection refers to the ability to assess and recognize goods and agents quality properties in the market. A classic example of the adverse selection problem is when people (buyers) who are high-risk buy health insurance. Since the insurance company (seller) suffers a lack of information about potential customers (due, for example, to privacy policies), it is not able to distinguish "good" customers from "bad" ones from the perspective of the insurer. In the context of illicit goods trading on the hidden places of the web, an example of adverse selection is represented by the situation where the buyer cannot directly compare products for which pictures, descriptions and feedback might be falsified. Vendors have more information about the goods they sell compared to their buyers. A buyer can only assess the quality of the drug after testing it. Hence a buyer might easily end up paying a larger price for a low quality product, due to the lack of meaningful information and assurance about the sellers and the traded items. Moral hazard refers to the problem of behaving in a more risky way than usual to gain an advantage, since another party is going to bear the cost of those actions. Hence an agent may decide to act in a risky way in order to gain higher benefits, given that the risk taken will not produce any losses for her/him. For instance, the platform administrator may exit scam their users, by stealing money held in their market account deposit.

An important point mentioned in [40] is that given the high turnover in such markets, regular buyers often have more than one supplier. The high turnover should reduce the value of searching for the "honest" vendor ("strategic games of repeated interaction"). This means that vendors should be encouraged to sell goods with lower quality than expected.

2.3.2 Trust and reputation

If on average is more profitable to sell low quality goods and cheat, why markets appear to survive and grow until LE take-downs? Again in [40] it is pointed out that despite the lemons can be very common and the turnover being very high, trust is of fundamental importance. Hence cooperation is going to prevail.

Trust between vendors, buyers and platform administrators is of crucial importance for the success and the durability of the market. In [40] the repeated game is taken into account showing the cooperation involves high quality actions. Even when cooperation is preferred, there could still be the chance that cooperation might be selective, in the sense the vendors may simply decide to scam some customers and keep good relation with other regular ones. One of the main difference between street and online dealing relies on the reputation and regulation mechanisms. Even thought those exists to a certain extent even in street markets, describing them is out of our scope. Instead, in online markets those can be directly identified. In [24] it is shown that the problem of moral hazard and adverse selection does not really affect the function of the market, thanks to reputation and regulation mechanisms such as ratings, feedback, reviews, content moderation, banning users and so on. In [24] reputation mechanisms are studied, figuring out that bad ratings actually lead to sales reductions and the seller is likely to leave the market. Their findings suggest that feedback mechanisms are important and crucial, as they provide more information to the parties involved into transactions of illicit goods, making it possible to achieve a certain level of trust. Buyers are able to check sellers' feedback given by other buyers and, at the same time, scammers and rippers can be banned from the platform, hence creating a more stable and safe environment.

Escrow payments Another way to mitigate (vendor) moral hazard relies on the use of third party escrow systems [24, 31]. An escrow is a financial arrangement between two parties involved into a transaction. A trusted third party holds the funds meant to be transferred to the seller until the buyer receives the purchased item or service (or if a specific period of time has elapsed and no complaints are made). In other words, buyer's money for a particular purchase are hold by the platform and released to the vendor only when the buyer notifies the correct shipping. This approach reduces the risk of fraud by the vendor, since if the buyer does not receive the item or the transaction fails, there is a third party that can handle the dispute and may refund the scammed user. Figure 2.1 shows the escrow process. However this approach introduces the problem of platform moral hazard [24]. In fact, market administrator can simply steal the money held into the escrow addresses under his/her control and leave the market. In other words, escrow systems have a single point of failure represented by the entity the holds and controls the money. This has happened several times in the history of illicit drug platforms. For instance, in 2016 the administrator of the marketplace Evolution exited-scam the users, stealing 12 million USD from the escrow systems [2].

Multisignature transactions A solution to the platform moral hazard raised by the use of escrow systems is the so called multisignature transaction, where funds can be released only when multiple parties involved in the trade agree. As in the escrow case, first money need to be deposited onto a dedicated address. This time, however, the address is cryptographically signed by all the

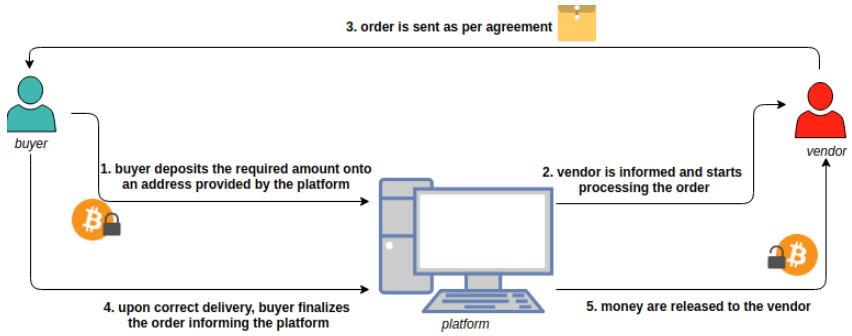

Figure 2.1: Escrow process

parties involved in the trade (in our scenario those are buyer, vendor and platform). In order to release the funds, multiple parties have to unlock the virtual safety box where money is held. Usually we consider 2-out-of-3 multisignature schemes, where at least 2 parties (for example, buyer and vendor) have to agree in order for the money to be released. In this way, platform exit-scam can be avoided, since there is no way to obtain the deposited funds without knowing the private key of (at least) one of the other parties. Figure 2.2 shows the case of a 2-out-of-3 multisignature transaction. Every participant needs to create a public key to secure the funds of their payments. With the correspondent private key it is possible to unlock the funds and release them to the correct entity. The set of public keys is used to generate the Bitcoin address, instead of depositing coins in a market-controlled wallet. Multisignature transactions systems make it very difficult to experience both types of moral hazard (vendor and platform). However they are hardly implemented, given the increased transaction costs involved [24] and the increased difficulty of setting up the procedure in the correct manner.

Finalize Early (FE) Finally some platforms also allow vendors to make use of the so called Finalize Early (FE) option. This is a transaction method that assure very fast order processing and payments, since money is not held in any escrow and no long confirmation waiting times are needed. After receiving the request for purchase, the platform waits for the vendor to label the order as "shipped" and then release the funds to him/her. In case of disputes, the platform has no way to refund money to the possibly scammed user. Therefore it is an advised method only when dealing for trusted vendors, who can gain advantage form this option since payments are received immediately even when goods are not shipped for any reason.

Feedback system Feedback systems provide a way to assess products and sellers properties on the market, giving users a better knowledge and thus, mitigating the effects of information asymmetry. Sellers are willing to provide quality products and avoid any kind of conflict, in order to receive good feedback which will increase their trading activities. In a study by Florencio et al. [26], the authors found some key elements which were the cause of market failures. The results suggest that without some sort of mechanisms, such as feedback systems, user trading and transaction history and the assurance on the actual existence of buyers and traders, the market is not able to be robust and functional. Reputation and regulation mechanisms are vital for the surviving of the market. In other words the durability of every illicit market is related

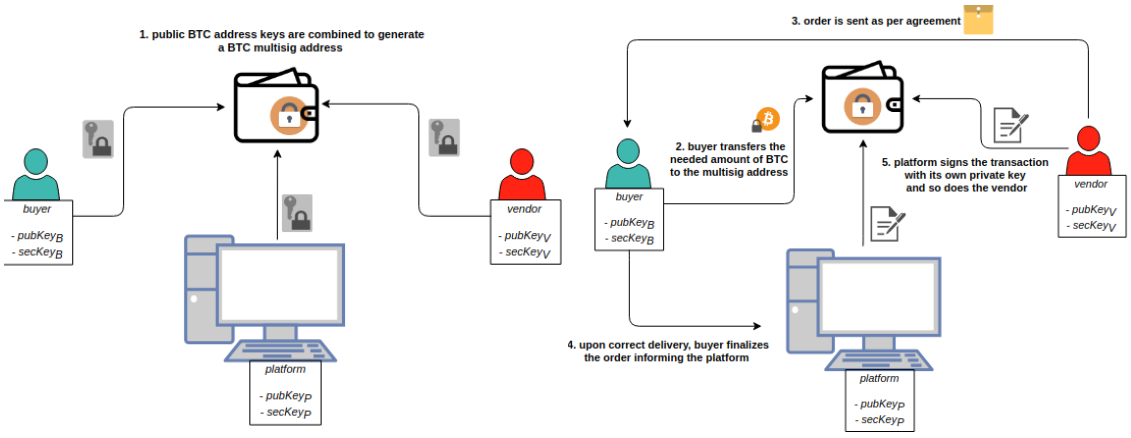

Figure 2.2: 2-out-of-3 multisignature BTC address creation and payment process

to the efficiency of trades, reliability of platforms and trust among agents through reputation and regulation systems. Allodi et al. discuss the reported findings of Florencio et al. in [21] and in their work they also compare the mechanisms of two illicit underground markets. They discuss the success and the failure of those markets, also taking into account the effectiveness of regulation mechanisms (i.e. the enforcement of rules, such as banning violators). In one case the analysis shows that banned users have (on average) a better reputation than normal users. If reputation system fails, there is no metric to distinguish between bad and good trader and therefore the market is likely to collapse and become inactive. Moreover they investigated the regulation system and found out that rules to punish violators were not corrected implemented. Concerning the other market under study, authors found that reputation and punishment mechanisms were correctly implemented and enforced, generating meaningful information for the user, yielding a functional trading system within the platform. In a previous work of Hardy et al. [32], it is shown that feedback mechanisms and reputation are sufficient for a functional market, which can exist without government regulation. The study was conducted on the Silk Road marketplace and the result of the investigation led to believe that reputation is necessary for the existence of the market. Moreover they found that sellers with higher reputation could charge premium prices. This process motivates sellers to provide quality goods and services. In [33] an emphasis is put on the role of feedback and reviews in stolen data markets. Also in this context rippers can cheat buyers given the large amount of information asymmetry in place. In fact, buyers can verify the quality of data only after they received it. Authors focus on signaling theory, trying to understand how criminals identify themselves to each other and signal trustworthiness. Authors analyze advertisements, which are the first form of signal presented by the vendor. Then the presence of negative feedback posted about a seller is a way to signal to other buyers the trustworthiness of a seller.

2.4 Underground e-marketing techniques

In this section we introduce the role of marketing techniques within the darknet trading activities. If on one hand the durability of every illicit market is related to the efficiency of trades, reliability of platforms and trust among agents through reputation systems, on the other the growth of the

market is related to the volume of trades and revenues. In legal markets those are usually achieved through marketing techniques.

Some evidence [19] show that marketing techniques may be employed in illicit markets, thus it is interesting to verify whether they adopt the same strategies of legitimate markets in terms, for example, of sponsoring a product, providing customers support or engage in affiliate marketing programs. In the report analysis it is mentioned that common marketing techniques, such as offering free samples of a product or offer discounted prices for loyal customers, are employed among market vendors, but an extensive analysis is currently missing.

Community forums are the place where that kind of advertising and sponsoring happen and, therefore, sellers are interested in keeping their advertised posts visible and with attractive contents. In [36] it is shown that membership discounts are offered to regular buyers to increase their loyalty creating a strong sense of community which can stabilize the market.

Vendors are also interested in promoting their brand, by creating a brand identity, with specific logos and pictures which can create a sense of trust and product quality into the customers. According to a research by Avast Threat Labs [10], the creators of the Petya and Mischa ransomware decided to establish a brand, the Janus Cybercrime Solutions. In order to increase sales and revenues, as for legal markets, they decided to create a brand logo and promote it even on social medias. Janus also engaged in its own affiliate marketing program, creating a professional payment system with whom the dark company could get a percentage of the profit the user would have earned.

Moreover banner adverts could be used and placed on search engine such as Grams [7]. Grams offered advertising for vendors via its TorAds and GramsWords [19], the dark counterpart of Googles "AdWords" and "AdSense". Gramswords allows vendors to purchase a "sponsored" area at the top of the search results, while TorAds allowed vendors to advertise on Grams and monetizing by offering space on their website. Launched in April 2014, it has been closed at the end of 2017 [12].

Chapter 3

Methodological approach

In order to address the research questions as defined in Section 1.3, qualitative and quantitative methods were applied, consisting of: direct observations of Darknet Markets features, case studies, examination of forum threads, automated collection, parsing and analysis of Darknet Markets data. In this section we explain the process and the criteria that led to the selection of a meaningful set of platforms to investigate. Moreover we list and describe the most significant pieces of information we obtained, focusing on features and aspects that might be important in the context of platform strategic differentiation and planning. A particular emphasis has been placed upon whether there are specific platform features that might drive players positioning in the underground environment. This study considers two aspects of the economics of illicit online drug trading. First, it offers an overview of the main markets operating in the underground, describing features and changes over the time. Second, it looks at whether these features play a role in the strategic positioning and decision making. Our aim is to correlate core problems of underground economy to DNMs features that are implemented to mitigate those issues.

3.1 Market sampling

The first step is to generate a meaningful sample of active and operating platforms. As we are investigating factors that can affect decision making on these platforms, as a sampling mechanisms we adopt two sampling criteria: platform visibility to the underground community and their volume, with regard to the number of users and, possibly, the magnitude of the profits made across different darknet markets. In the following paragraph the main sources of information are described, followed by the discussion of the chosen criteria and the results of this sampling approach.

Sources For the purpose of this study, we consider only darknet markets that operate as Tor hidden services, excluding single vendor websites. Initially we surveyed the underground ecosystem by manually collecting notes and data. By doing this we identified and surfed the main sources of information and search engines that index Tor onion URLs. There are several results that can be found on clearnet or only via Tor network. An exception is DeepDotWeb.com, one of the most popular news website about the darknet ecosystem with reviews, interviews, blacklisted markets

forum	activity	description
The Hub	since January 2014	cross-market sections and threads, new marketplaces area
Dread	since April 2018	Reddit-style, relaunched in May 2018 after being unavailable for some weeks
DNM Avengers	since 2015	harm reduction, discussion and lab testing of drugs

Table 3.1: Three of the most popular darknet forums and user communities

and comparison charts (still up and running at the time of writing). That website is available also as Tor Hidden Service, making it more appealing for users who want to do their research while being assured of a certain level of anonymity and identity protection. During this research study, that website appeared first or second when querying Google.com or DuckDuckGo.com. We argue that it may represent one of the likely source of information that most newbies (but also expert) use to gather information, news, updates and, more importantly, verified and reviewed links to marketplaces. Whereas on clearnet sources (such as disinterment's.org and darkwebnews.com) several reported scamming websites are listed, DeepDotWeb policies make it quite difficult to add a totally untrusted and likely scamming site to their list. As a result most of the websites that are not listed on DeepDotWeb are likely to be not to investigate on, given their scarce reliability in terms of meaningful source of data. On the other hand, markets listed and reviewed on DeepDotWeb (and that are also present on other websites) appear to be active and they are topic of discussions on underground forums and clearnet Reddit communities. DeepDotWeb also reports a list of three verified discussion forums, shown in Table 3.1. The Hub seemed to be the most suitable discussion forum to analyze in order to gather meaningful information. The new marketplaces section turned out to be very useful for collecting some insights about the trends and the advertising behavior of new darknet markets owners.
Summarizing, main sources of information considered are:

- DeepDotWeb (both on clearnet and on Tor): the most popular news website about the darknet ecosystem with reviews, interviews, blacklisted markets and comparison charts (still up and running at the time of writing).
- TheHub (only on Tor): one of the most popular discussion forum, with several sections, one dedicated to new emerging marketplaces(closed since April 2018, apparently back online during August 2018). Both constitute the largest source of information on DNMs, after the Reddit community was banned.

At the moment of writing there were more than 30 markets advertised and, possibly, linked by the above-mentioned sources. We sampled the DNMs ecosystem in order to consider only those markets that are actually active and whose users makes purchases and generate revenues. The following paragraphs describe the sampling approach and its results.

Sampling criteria Our study focuses on underground drug trafficking on popular, successful and promising darknet markets. The analysis process is driven by data obtained through direct observations and automated scraping of platforms in order to acquire information about strategic marketing techniques, particular features that the platform offer to attract customers and revenues generated. A priori we excluded vendors private web shops for which such information is not available or features (such as rating systems) are simply not implemented, given the direct nature of the business and absence of competitors on private vendors sites. The first step of the analysis

consists of defining a market classification, which may help clustering markets in groups that share similar characteristics. We chose visibility and volume of the market as criteria for our markets classification.

The visibility criterion addresses the ease of finding and accessing the market for the average user. Here with average users we intend potential market participants who are willing to join a market, listed and advertised on one of two sources defined above. The attribute "average" is meant to pursue the idea of a not so technically skilled or expert user.

DeepDotWeb is one of the largest source of information about Dark Net Markets. Thanks to its high amount of articles, news, markets descriptions and comments, it provides significant guidelines to any user who is approaching the underground community. Moreover it is accessible both via clearnet and via Tor network, thus likely being the potential first landing place of interested (or just curious) users. These characteristics give high visibility to the platforms listed on DeepDotWeb, while posts on TheHub needs a basic understanding of how to connect to the Tor network and the ability to find the correct onion link. Hence although markets with little or no popularity on DeepDotWeb might be listed on TheHub, they are considered to have a smaller visibility.

The volume criterion refers to the amount of trades in the market. Having a real estimate of this attribute poses lots of challenges. Above all it can be properly addressed only through a quantitative reliable analysis of exchanged data, which is far from being extensively available. However we argue that by investigating forums threads, sources, news and literature, it is possible to distinguish and select markets that experience a larger number of participants, listings and revenues.

Classification and categorization Given two attributes (visibility and volume) and two categorical distinct values (high and low) we try to classify darknet markets into four tiers, as depicted in Table 3.2. Tier 1 consists of the top three markets listed on DeepDotWeb; Tier 2 is the set of all the markets listed on DeepDotWeb, excluding the ones in Tier 1; Tier 3 is the result of the selection of the most prominent new marketplaces on TheHub, which are not advertised on DeepDotWeb or among the top three platforms on TheHub itself. Finally Tier 4 represents the set of markets resulting by taking the top three markets listed on TheHub, which are not listed on DeepDotWeb. Tier 4 is defined in such a way that no markets were found to meet high volume and strictly low visibility requirements. In other words, we did not find a platform with lots of customers and listings which was not already present in the first three tiers

Selected markets The classification process yielded the selection of twelve different operating markets, shown in Table 3.3. Those platforms have been investigated for an overall period of 6 months, from February till August 2018. However during the research process, some markets became unavailable. In particular Libertas and Zion Market (tier 2) and Apollon Market (tier 3). Therefore the study has been conducted mainly on 9 platforms operating during the last 6 months.

		Volume	
		High	*Low*
Visibility	*High*	Tier1	Tier2
	Low	Tier4	Tier3

Table 3.2: Tiers

Tier	DNMs	# listings	% drugs
1	Wall Street Market	11000	49%
	Dream Market	130000	46%
	Point / Tochka Free Market	5100	67%
2	Olympus Market	32000	58%
	Libertas Market	n/a	n/a
	CGMC Market	1850	100%
	Berlusconi Market	17000	48%
	Zion Market	n/a	n/a
3	Apollon Market	n/a	n/a
	Empire Market	4500	30%
	Rapture	4000	46%
	Serpent	n/a	n/a

Table 3.3: Sampled markets under study

3.2 Qualitative data collection

The aim of our qualitative research was to derive an overall picture of the DNMs ecosystem where the most popular and promising emerging markets are acting. The results of the analysis give insights about the existence of particular features which may drive actors behaviors and choices with respects to the core problems of adverse selection and moral hazard. Qualitative data collection process was based on two different approaches: 1) direct observations and 2) analysis of case studies. By directly observing and collecting platforms characteristics and relating our observations to the literature discussed in 2.2 we identified four macro-criteria which may constitute a starting point for decision making. Analyses of case studies involved daily reading of articles reporting news, interviews and law enforcement activities and investigating users feelings and thoughts by analyzing dedicated forum threads.

3.2.1 Attribute of interests

In order to understand if there is any rationale behind the choice of a particular trading platform, a particular focus was given to factors that may influence vendors and buyers decisions. Forum threads, comments and feedback, together with news articles and tutorials, form a significant set of sources to gather feelings, hot topics, concerns, and issues among buyers, vendors and platform administrators. In the remaining of this section we discuss which factors and features we found interesting in order to build our analysis on them.

Security design of market platforms Darknet markets platforms (websites and forums) offer a typical and intuitive layout, similar to any e-commerce website. Given the illegal setting and the necessity to use anonymizing technology, such as the Tor browser, there are some security concerns which platforms may address, proposing and implementing security countermeasures to avoid misuse and attacks. Security is an important concern for every player in the game. For

our analysis we gathered information about login and access methods, (un)availiablity and load issues, confidentiality of sensitive data, phishing attacks countermeasures and potential security vulnerabilities. Security implementations should face the problem of moral hazard posed by the platform, given the risk the users undertake when trading in an unsafe environment.

Payment techniques In addition transactions methods play an important role. Hence we focused on cryptocurrencies used and transaction methods implemented. Advanced and secure payment methods can mitigate the problem of moral hazard posed by the vendor or the platform, since money can be released only after certain security conditions are met.

Vendor bond The fee a vendor has to pay in order to sell and trade on a platform may represent a weak signal of moral hazard problem, given the commitment the vendor is taking to the platform, putting at risk his/her anonymity and funds.

Marketing techniques Being e-commerce platforms, those platforms may offer affiliate marketing campaigns, sponsorship, awards for loyalty, bulk discounts, and various forms of advertising. More knowledge and advertising is available, less information asymmetry is faced. Thus those mechanisms might be used and mitigate adverse selection problems.

Buyers statistics and type of products We also looked at the presence of buyers statistics and information (useful feature for vendors) and the product diversification of offered listings. Those mechanisms can face the adverse selection problems, shaping those reputation systems discussed in Chapter 2.

3.3 Quantitative data collection

The goal of our quantitative data collection was to give numeric support for our qualitative interpretations. Moreover by comparing our findings with results reported in the literature (e.g. with regard to the number of active vendors or the magnitude of sales in a timespan) it was possible to assess the state of the art of the new selected markets.

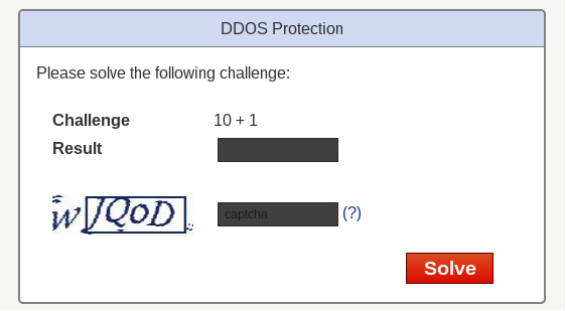

Figure 3.1: Dream Market DoS protection mechanism

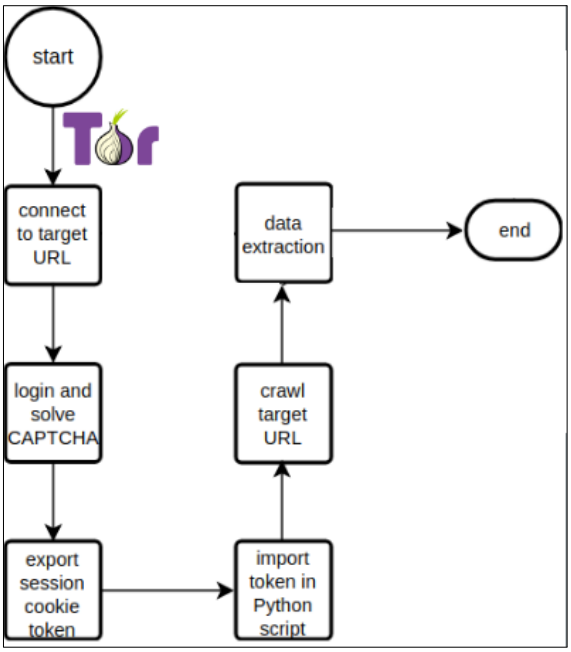

Figure 3.2: Scraping process

3.3.1 Crawling and scraping Tor onion sites

DNMs platforms relies on authentication cookies that can be reused for few days (sometimes up to a week). However DoS protection mechanisms are implemented (for example in Dream Market, as shown in Figure 3.1) and even while keeping the same connection cookie, some websites ask to login and/or solve a new CAPTCHA. Therefore whenever connection errors are raised or protection mechanisms are triggered, the script ends running and a manual intervention is needed to access the website again. The process flow is depicted in Figure 3.2. For each of the three markets we developed an ad-hoc web crawler, scraper and data parser. Given the different structure of HTML pages and different text formatting between websites, post-processing of data was also needed. The scripts are written using Python 3 within the PyCharm IDE. In order to connect to a DNM platform, the Tor service must be up and running on the operating machine. Usually Tor service runs on port 9050 (as in our case) or 9150. Port number is essential since all the TCP traffic directed to that port will be sent over the Tor network by using a local proxy (SOCKS). By using the Python request module, it is possible to send a get request to a particular website, specifying its URL, proxies and the cookies used in the request. In order to get a valid cookie which can be used to maintain a session over the same Tor circuit allowing for multiple consequent requests without connection dropping, we manually access the target onion URL using the Tor Browser. Then we manually resolve the CAPTCHA and then record the cookie value sent by the server through the developer console. Once connection is established and maintained through a valid cookie is it possible to start scraping the target onion site. When too many requests within a short timespan are made, some platforms may exhibit some anti-DoS feature, by asking to manually solve another CAPTCHA and/or an addition.

In general, DNMs scraping posing some challanges which may affect the results of the analysis. First of all the are slow to crawl and availability of data is not always guaranteed, such as its

timespan	platform	data	# files	size (MB)
02/06	Berlusconi Market	all drugs listings	453	29
		vendors' info, feedback and products	1148	33
03/06-04/06	Dream Market	vendors' info, feedback and products	3342	296
06/06	Empire Market	all drugs listings	95	5
		vendors' info, feedback and products	532	14
06/06	Olympus Market	all drugs listings	280	41
		vendors' info, feedback and products	442	17
29/06-30/06	Berlusconi Market	vendors' info, feedback and products	1192	36
30/06-03/07	Dream Market	vendors' info, feedback and products	3492	500
19/08-20/08	Dream Market	feedback	1846	253

Table 3.4: Scraping information

vendor	PGP key id	visible sales	tot €	€/sale	share	FE	join date
CHEMIST	0xE1DB437A	300	21660.0	72.2	0.07%	Yes	21-9-2016
Mr.Erection	0xB11E2A97	300	13125.0	43.75	0.04%	Yes	19-5-2016
dutchglory	0x42960549	300	15395.0	51.32	0.05%	No	21-8-2017
JuicyLucy	0x361CA7CF	11	285.0	25.91	0.00%	No	10-5-2018
DUTCH2GO	0x5831CD69	291	5899.0	20.27	0.02%	No	2-3-2018
thepostmanpat	0x066FB0A8	300	18245.0	60.82	0.06%	Yes	2-2-2018
OXY-CONNOISSEUR	0x97B8C250	118	18059.5	153.05	0.06%	Yes	28-9-2017
Tony_Montana	0x4E7EF339	300	95538.0	318.46	0.32%	Yes	26-6-2017
toptierdrugs	0x2E267412	300	68250.0	227.5	0.23%	Yes	22-10-2016
XanaxBlotters	0xF12B5CE5	300	28014.5	93.38	0.09%	Yes	25-1-2018

Table 3.5: An excerpt of the dataset

reliability. Session cookies may not be kept for long for all the websites and the HTML structure of web pages may change over the time.

3.3.2 Datasets

Data collection details are reported in Table 3.4. The first snapshot produced a datasets containing 2302 rows and 10 columns (market name, vendor name, PGP key ID, visible sales, revenues, revenues per sale, market share, Finalize Early (FE) option, join date, product types). Every row represent data of a vendor on one of the 4 markets. Thus our initial dataset included 2302 vendors. At the same time we found 1964 unique PGP keys. Therefore some vendors use the same PGP key on different markets. For each vendor we recorded the market where she/he operates, PGP key ID, number of visible sales (i.e. number of feedback, each of which associated to an order and its price), revenues (converted in EUR), revenue per sale, market share, finalize early (FE) authorization, join date and product types. Some platforms make available all the sales made (with the related price), while some others report only the given feedback without mentioning the cost of the purchase. As an example, in Table 3.5 the first ten rows of the dataset related to Dream Market are shown. The largest number of sales shown is at most 300 for each vendor.
In the remaining of this section extracted data is described.

Vendor profile Some vendors operate on more than one market, sometimes using the same name and the same PGP public key as a proof of authenticity. In some cases, vendors also open multiple accounts on the same market, although they are expected to pay a vendor fee for each of them, which may be costly.

Vendor revenues DNMs do not make publicly available the revenues of their vendors. Instead only (a fraction of) the feedback are reported. However, each feedback is linked to a particular sale, for which the price is shown. Thus, it is possible to have an estimate of the revenues made with a certain number of sales (i.e. number of visible feedback).

Listings information DNMs allow vendors to categorize their listings using a preexisting set of categories. Among markets the name and sub-sets of listings may change, rising the need for data post-processing. In particular, every product type found for a vendor was mapped to a standardized name following a custom categorization scheme (e.g. "hash/oil" -> "Cannabis&Derivatives").

Chapter 4

Comparative qualitative analysis of markets

4.1 Exploratory analysis of sampled markets

In this section the results of our exploratory analysis on selected Darknet Markets are discussed. First we provide a description of the features and functionalities of each sampled DNM and then we summarize the findings. The focus is given to those features that might be employed to mitigate moral hazard and adverse selection problems.

Dream Market

Overview Dream Market is the oldest active DNM at the time of writing. It was launched as a Tor hidden service in late 2013 and at the time of writing is one of the largest markets, after the shutdown of Hansa and Alphabay. The layout and user interface are very simple. Buyers can search for vendors with a "trusted vendor" label, which is acquired when a significant history of successful transactions and positive feedback are reached. In order to purchase goods buyers have to deposit digital coins to their own Dream Market wallet. The accepted cryptocurrencies are Bitcoin (BTC) and Bitcoin Cash (BCH) to increase transactions anonymity, and Monero (XMR) for improved privacy and untraceability. Usually the deposit process requires about 30 minutes and 3 confirmations from the network before being approved. Dream Market uses a traditional escrow method to avoid vendors scams. However it lacks the anti-platform-scam protection given by a multisignature system. After the purchase is made and the package is received, buyer can finalize the order so that money in the escrow are released to the seller. Then buyer can leave a feedback regarding his/her purchase. Transaction fees for withdrawal are quite important: 0.00015 BTC + 0.5% of the withdrawn amount; while commission rate for sales is 4%. Vendor application requires to pay a bond of 0.1 BTC, which is refundable after closing the account, after reaching a significant transaction and feedback history or after providing enough trading history on other platforms, such as PGP verification of previous accounts. The Finalize Early (FE) payment method is only allowed for verified vendors and after receiving permission from support. Finally direct deals/payment (DP) are not permitted. Dream Market does not provide

any buyer statistics and their feedback are anonymized. There is no information about a particular buyer from a vendor's perspective. On the other hand, platform provides a dual rating system to increase trust in vendors. The system is significant for well known and established vendors. Indeed, average scores and number of positive and negative feedback on other markets (where the seller has been active) are shown, thus increasing the information available to the buyer. The affiliate rate profit made through the use of referral links is 25% of the commission fee (%4). This means that every recruiting user can earn 1 USD every 100 USD spent by the recruited user. Since 2016 Dream Market also supports a bug bounty program, rewarding 75 USD for every security vulnerability or bug discovered.

Security Dream Market uses standard login and security features: password only, PGP only, 2FA, optional extra security password or PIN for purchases, last login information and PGP verified trusted mirrors. However a deeper look and research into this platform revealed some potential security vulnerabilities, which may be exploited and put users at risk. The first potential issue is that Dream Market uses JavaScript code. If no client protection is taken (i.e. disabling JavaScript in browser), JavaScript files are downloaded when accessing the website. We found that one of them, market.js, contains a clearnet IP, which seems to redirect to a script written in Ajax and directly hosted on the main IP address (see Figure4.1). Another clearnet IP is also present in the index.HTML file in the form of a comment, as shown in Figure4.2). The exposures of IP addresses were already found and reported in 2017 [3], and still there is no mitigation or solution to problem. In addition, Dream Market clearnet (deepwebnetwork.com) and onion forum have been analyzed. The former contains monitoring scripts (Google analytics) and the domain lookup reveals the hosting platform (GoDaddy.com, LLC service provider from USA) and the registrant name (apparently from NL), while the latter shows its IP address in the http response header (196.44.177.237, from Zimbabwe). This presumably discloses the actual location of the web server or of the used VPN. Reverse IP lookups have been performed using viewdns.info web service and the results are reported in Table4.1.

Overall Dream Markets does not experience high level of trust from the underground community. Users complaints and negative reviews indicate a series of recurrent scamming incidents that affects platform reputation, such as phishing scams, fake goods, non-delivered orders and unusual banning of sellers with their consequent loss of money [4]. In addition the fact that Dream Market is the longest-running platform since the main law enforcement operations, it is continuously reported to be a strategic honeypot to monitor and control user activities in the long run. Indeed lately quite few arrests of vendors operating on dream market have been reported. However Dream Markets is still an important actor in the game, accounting for large revenues and a significant number of vendors and customers, despite the security problems, concerns and the absence of appealing features to prevent scams and promote harm reduction and quality control.

Wall Street Market

Overview Wall Street Market is operating since 2015. It offers around 11000 listings, for which drugs represent around the half of the total. Vendor application is free of charge for trusted vendors that can show proof of their past activity. Otherwise the basic vendor account fee is

ip	file	hostname	country	domains hosted
143.95.243.239	index.HTML	dallas137.arvixeshared.com	USA	108
194.9.94.82	market.js	iis12.windowscluster.loopia.se	Sweden	185
160.153.75.41	clearnet forum http response	ip-160-153-75-41.ip.secureserver.net	USA	119
)5-5 196.44.177.237	onion forum http response	h237-vamizi.yoafrica.com	Zimbabwe	0

Table 4.1: Reverse IP lookup of Dream Market leaked addresses

Figure 4.1: Dream Market HTML and JavaScript files

```
function updateBuddyList() {
        var debugUrl = "http://194.9.94.82/ajax?t=chat&c=buddies";
        var usedUrl = useDebug ? debugUrl : "./ajax?t=chat&c=buddies";
        ...
```

Figure 4.2: Dream Market IP leak from market.js

```
        </div>
    <input type="hidden" name="32bc93cd66139f0cd901167b16b9b62c" value="291a91f86a89731ab7a876724949f7b8">
    <input style="display: none;" name="daf60f766f49e4b67f5a58b267c2150a"
        value="archerfishguaranteed"/>              <div class="captcha">
        <label> </label> <img class="captcha3"  src="img/captcha3" alt="Captcha">
        <!--
        <img class="captcha3"  src="http://143.95.243.239/img/captcha3" alt="Captcha">
         -->
    </div>
<div style="font-size: 12;">Please enter the 4 letters surrounded by the box (case sensitive).
Please check always that you are on the correct url.</div>
            <div>
    <label for="b40904ff390f4bef7a45baa1a6a8a92b">Captcha code <a href="./help#UsingCaptchas" target="_blank" >(?)</a></
    <input id="b40904ff390f4bef7a45baa1a6a8a92b" class="text   "
        name="b40904ff390f4bef7a45baa1a6a8a92b" type="text" title="Captcha, case sensitive"/>
</div>
<div class="actionContainer iro845uireu73reutr8"  style="display: none;" >
    <input type="submit" value="Login" name="4a277d1d9d99f02c2d0474b93059448a"/>
</div>
```

Figure 4.3: Dream Market IP leak from index.html

150$ (restricted to multisignature and escrow) and the professional account reaches 500$ (with no restrictions).

The main difference with Dream Market is that buyers do not need to deposit money into their platform account first and wait for confirmations until purchasing is enabled. In order to purchase goods buyers just have to deposit digital coins to an address created by the platform, that will held the funds. When the buyer finalized the order, the money is released to the vendor. Wall Street Market implement also a "finish early" payment method. It is a form of direct pay (DP) where coins are directly sent to the vendor. Usually it is a unadvised practice, since the platform cannot have any role in case of disputes. One of the advantages is that buyers can use this method when buying from trusted vendors and the same time exploiting any changes in the Bitcoin price. For instance, buyers can decide to buy a particular good when the price of the cryptocurrency decreases. Finally a 2-out-of-3 multisignature scheme is in place. The platform's key will be used to release coins to the seller or to refund the buyer. The platform also implements some features, such as an award system for some taken actions. For instance there is an award for using Multisignature transactions or escrow methods a given amount of times and an award for purchasing different product from different categories. Awards are shown as badges on a user profile web page and may give more information and context regarding, for example, a particular vendor and his/her activity on the market.

WSM provides a simple level system for vendors. Based on the level there are different commission fees. Vendors and buyers with an high level are likely more trusted than others. Levels are based on the amount of EXP points a user has. Those can be earned, for example, when receiving a positive feedback, by successfully completing an order, by recruiting users via referral links, or can be lost when receiving a negative feedback. Levels range from 1 (with 5.5% commission rate) till 15 (with 2% commission rate). The affiliate rate profit made through the use of referral links is 25% of the commission fee (%4). This means that every recruiting user can earn 1 USD for every 100 USD spent by the recruited user. Since 2016 Dream Market also supports a bug bounty program, rewarding 75 USD for every security vulnerability or bug discovered. The affiliate rate profit made through the use of referral links is 20% of the commission fees (2-5.5%). This means that every recruiting user can earn from 0.4 USD up to 1.1 USD for every 100 USD spent by the recruited user. An interesting feature of Wall Street Market is the quality control partnership with DNMAvengers, a forum for laboratory testing of small samples of drugs for harm reduction purposes. However it is not the first crypto-drug harm reduction service. In 1997 in Spain Dr. Fernando Caudevilla started Energy Control, which became the International Drug Testing Service 2014, with testing fees of 70 up to 120 for a detailed report and the guarantee of confidentiality and anonymity. This partnership creates a way to review substances and vendors, which makes it hard for scammers and cheaters to get unnoticed. On the DNMAvengers forum is possible to create tickets for report, which are evaluated by the staff. If the substance is tested, results are publicly made available. Finally the platform makes buyer statistics available, thus allowing vendors to have an overview on the entity they are selling to.

Security As a set of basic standard features, Wall Street Market implements password only and 2FA login methods, last activity information to avoid phishing attacks, together with verified URL with PGP signature updated every 2 weeks. It has been reported that the platform

exposed an IP address during a downtime in October 2017 [15]. The Reddit user DNSecurity-Consultant revealed that "Wall Street Market's IP address is 62.138.14.136 and the hostname is loft24104[.]dedicatedpanel[.]com.". In the same time also a Twitter user found another clearnet IP (185.35.139.36) linked to the platform [14].

Point / Tochka Free Market

Overview Point / Tochka Free Market was started in 2015 by Russians developers. It differentiates itself from the others through the adoption of instant trade and quick shipment features. Buyer and vendors do not need to communicate directly. Moreover it is the only markets which considers "dead drop" shipping methods for vendors. This platform relies on open source code and hardened security.At the time of writing it is the only darknet market supporting Ethereum (ETH). Point/ Tochka provides 7 days escrow system and 2-of-3 multisignature transactions. Founders claim 160000 users, 10000 vendors, 25000 listings. However those numbers are far from the actual estimate. The platform suffers from few vendors and listings, despite the arguable number of registered users. The main types of trade goods are related to prescription, pharmaceutical drugs and opioids. Tochka is self-described to be an Independent research organization in counter-economics (Digital Shadow Economy) with the plan of *develop a system for managing reputation and allowing decentralized logins on blockchain*, that is a sort of Google Login for darknet. Moreover they claim to make use of Zydeco smart contract for company dividends, making the overall organization looking serious, committed and professional. They provide the highest affiliate program profit (up to 45%) and a vendor fee below the average (up to 200 USD). As for Wall Street Market, they have a quality control partnership with DNMAvengers. Tochka utilizes vendor level system to improve the quality and reliability of feedback, trades and overall system. For instance 10 successful deals correspond to 1 level, while 6 months on the marketplace award a 2x multiplier for increasing levels.

Security Tochka is an open source code project under the MIT license.To the best of our knowledge there are only two security issues found. First, for a short period of time Point Market was running a clearnet website on which onion mirrors were published in case of DoS attacks on the hidden server. Then in October 2017 a Reddit user reported an IP address exposure.

Olympus Market

Overview Olympus Market provides around 32000 listings for which drugs accounts for more than the half. Vendor application is free of charge if past activity history is shown. Otherwise the bond is 0.03 BTC. It offers a traditional escrow system and a 2-out-of-3 multisignature transaction method. On withdrawal there is a standard fee of 0.00000295 BTC. The affiliate profit rate is 25%. Monero (XMR) is also supported.

Berlusconi Market

Overview Berlusconi market is a classical escrow market with direct deposits, without the need of a wallet. All payments are sent directly from the users own wallet to the sellers wallet. The market does not implement multisignature transactions, instead only a classic escrow system is in

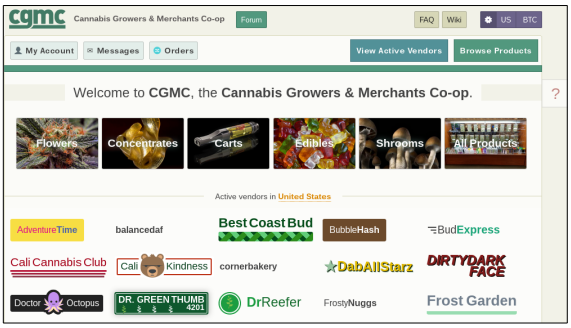

Figure 4.4: CGMC homepage

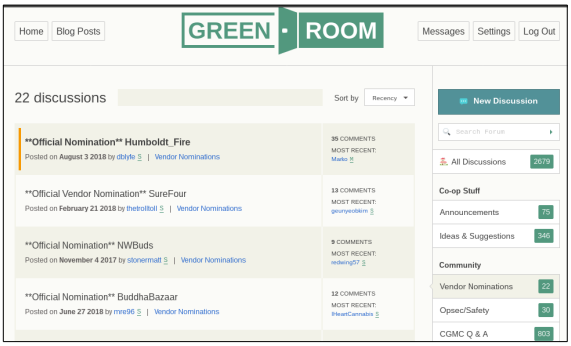

Figure 4.5: CGMC discussion forum

place (as in the case of Dream Market). The vendor bond is free of charge when proof of successful past sales is provided, otherwise the price is 0.034 BTC (refundable if the account is deleted or vendor becomes trusted). Buyer statistics are not available and no affiliate campaigns are offered. Moreover there is no partnership with the quality control service. It supports Monero (XMR) for better untraceability of transactions, Bitcoin and Litecoin (LTC).

Security As basic security features, Berlusconi market implements password only or 2FA login methods and the use of a PIN for withdrawal. Against phishing attacks, only a list of mirrors is provided.

CGMC Market

Overview The Cannabis Growers and Merchants Cooperative (CGMC) is a private, invite-only marketplace operating since June 2016. This market differentiates from the competition, by offering only cannabis derivatives and, for a very small part (less than 1%), psychedelic mushrooms. It comes with a very well done Wiki section and a dedicated forum, resembling a social network interaction among users. Figures 4.4 and 4.5 show the layout of the platform. Overall CGMC is a quite small cannabis-specialized market, with less than 2000 listings and less than 60 active vendors. Joining the platform requires an invite code, which is sent upon request after 5 days. Vendors are carefully screened and reviewed before being allowed to trade on the platform. CGMC allows direct pay (DP) payments, that is the equivalent of finalize-early (FE) on other markets: the payment is sent directly to the vendor. Multisignature transaction are also supported and re-

tier	platform	login methods	inbox encryption	optional password	withdrawal	phishing
1	Dream Market	Password only, PGP only, 2FA	enabled by default	yes (also for buying)	optional security password or pin	last login info, PGP verified mirrors
	WSM	Password only, 2FA	not implemented	no	pin	last activity info, url PGP signature
	Tochka	Password only, 2FA	not implemented	no	?	?
2	Berlusconi	Password only, 2FA	not implemented	no	pin	only a list of mirrors
	Olympus	Password only, 2FA	not implemented	no	pin	last login info
	Zion					
	Libertas					
	CGMC	Password only, 2FA	not implemented	no	?	?
3	Apollon					
	Empire	Password only, 2FA	not implemented	no	pin	?
	Rapture	Password only, 2FA	not implemented	no	pin	verified market links
	Serpent	Password only, 2FA	not implemented	no	pin	?

Table 4.2: Markets comparison based on security features

tier	platform	cryptocurrencies	FE/First/Direct	escrow	multisig
1	Dream Market	BTC, BCH	only for verified vendors	classic escrow	no
	WSM	BTC, XRM	allowed	classic escrow	2-out-of-3
	Tochka	BCH, ETH	allowed	classic escrow	2-out-of-3 for premium vendors
2	Berlusconi	BTC, XRM	allowed	classic escrow	not implemented
	Olympus	BTC, XRM	allowed	classic escrow	2-out-of-3
	Zion				
	Libertas				
	CGMC	BTC, LTC	direct pay	not implemented	2-out-of-3
3	Apollon				
	Empire	BTC, LTC, XMR	barely allowed	classic escrow	2-out-of-3
	Rapture	BTC, XRM	allowed + direct deal	classic escrow	2-out-of-3
	Serpent	BTC, XRM	allowed	classic escrow	2-out-of-3

Table 4.3: Markets comparison based on payment methods

commended. It supports Bitcoin and Litecoin and escrow commission is 2.5%. Buyers information and statistics are available after receiving the order. Finally it does not implement any affiliate or partnership campaign, leaving the overall marketing advertisement and managing within the community itself.

Overview of Tier 3 DNMs Empire, Serpent and Rapture markets are very new platforms which share the same characteristics, offering both a classic escrow and a 2-out-of-3 multisignature systems.

Empire market has a very low vendor fee (100$) and makes buyer statistics available (disputes, activity, completed orders). Rapture market's fee is of 250$ (free with proof of sales) with a fixed commission on withdrawal (0.17 - 0.5 USD) and 10% profit for every recruited user (affiliate program). It also offers a direct deal function for trusted vendors. Similar features are found in Serpent market, where the vendor bond is equal to 225$ (refundable with proof of sales), and profit for affiliate campaigns from 10 to 20% of the commission on recruited users' orders.

tier	platform	vendor application	level system	commission	buyer info
1	Dream Market	free (with proof of sales) or 0.1 BTC (refundable)	no	4% on order; 0.00015 BTC + 0.5% on withdrawal	no
	WSM	free (trusted), 150(*basic*)*or*500 (pro)	EXP points	2 - 5.5% on order	yes (disputes, activity, completed orders)
	Tochka	free (trusted), 100(*premium*)*or*200 (premium+)	yes	2 - 5% on order	no
2	Berlusconi	free (with proof of sales) or 0.034 BTC (refundable)	no	?	no
	Olympus	free (with proof of sales) or 0.03 BTC	yes	0.00000295 BTC on withdrawal	no
	Zion				
	Libertas				
	CGMC	invite only (or proof of sales) + community approval	no	shipping or escrow commissions (2.5%)	only visible for vendors
3	Apollon				
	Empire	100$ (or free with proof of sales)	yes (vendor level and trust level)	0.0003 BTC on withdrawal4% on order	yes
	Rapture	250$ (or free with proof of sales)	no	0.17 - 0.5 USD on withdrawal	no
	Serpent	225$ (or free with proof of sales)	yes (trust level)	0.50 % + mining fee on withdrawal	no

Table 4.4: Markets comparison based on agent selection features

tier	platform	affiliate campaign	quality control	quest rewards
1	Dream Market	25%	no	no
	WSM	20%	yes (DNM Avengers)	yes
	Tochka	up to 45%	yes (DNM Avengers)	no
2	Berlusconi	no	no	no
	Olympus	25%	no	no
	Zion			
	Libertas			
	CGMC	no	no	no
3	Apollon			
	Empire	20%	no	no
	Rapture	10%	no	no
	Serpent	10-20%	no	no

Table 4.5: Markets comparison based on and marketing features

Tier	Marketplace	bond	vendor status	commission	refundable	need proof
1	Wall Street Market	0	Vendor (trusted)		o	x
		150 $	Basic		o	o
		500 $	Pro		o	o
	Dream Market	0	Vendor		o	x
		0.1 BTC	Vendor	4%	x	o
	Point / Tchka Free Market	0	Free		o	?
		100 $	Premium	5%	o	o
		200 $	Premium+	2%	o	o
2	Olympus Market	0.03 BTC				
	Libertas Market					
	CGMC Market		Vendor			x
	Berlusconi Market		Vendor			x
	Zion Market	0.02 BTC	Lite	8%	o	o
		0.04 BTC	Regular	5%	o	o
3	Apollon Market	0	Vendor		o	x
		100	Vendor		o	o
	Empire Market	0	Vendor		o	x
		100 $	Vendor		o	o
	Rapture	<250 $	Reputable Vendor		?	x
		250 $	Vendor		x	o
	Serpent	<225 $	Well-known Vendor		?	x
		225 $	Vendor		x	o
	Cannazon	250 $	Levels (12 - 1)	2.25 - 5%	x	x

Table 4.6: Vendor application

4.2 Summary of findings

In this section we summarize our findings. The first exploratory analysis is depicted in Table 4.7. An overview of the discussion is also shown in Tables 4.2, 4.3, 4.4, 4.5 and 4.6. We found that vendor bond, security features and payment methods may address moral hazard problems, while partnership marketing and availability of information about vendors and buyers are used to mitigate adverse selection issues. We did not find convincing qualitative evidence of significant differences between market mechanisms across tiers. A different grouping could reveal hidden patterns, but from the perspective of the potential customer joining the communities (reflected as discussed in the adopted sampling criteria) no clear pattern emerges. In general, all the considered platforms show mechanisms and features that may mitigate adverse selection problems, by providing, for instance, information about vendors and feedback. Moral hazard may also be mitigated by the adoption of "more secure" payment methods (e.g. 2-out-of-3 multisignature transactions). Our investigation reveals that most successful platforms do not seem to invest and

		adverse selection								moral hazard							
		anti-phishing	PGP	level	awards	buyer info	feedback	cross verifiable	partnership	BTC	BCH	LTC	XMR	ETH	FE	Multisig	vendor bond
1	Wall Street	x	x	x	x	x	x		x	x			x			x	$150
	Dream Market	x	x				x	x		x	x		x		x		$700
	Tochka		x				x		x	x	x			x	x	x	$100
2	Olympus	x	x	x			x	x		x			x		x	x	$300
	Libertas		x				x						x			x	
	CGMC		x			x	x									x	
	Berlusconi	x	x				x	x		x		x	x		x		$400
	Zion		x				x			x			x		x	x	$300
3	Apollon	x	x	x			x			x							$200
	Empire	x	x	x		x	x			x		x	x		x		$100
	Rapture	x	x				x			x			x		x	x	$250
	Serpent		x	x			x			x			x		x	x	$225

Table 4.7: Exploratory observations

rely on advanced security features and improved payment methods, while less popular (but emerging) markets seem to focus on providing a more customer-centric environment (e.g. by providing buyers information and more controlled vendor applications), combined with advanced payment methods.

4.2.1 Mechanisms addressing moral hazard

Moral hazard problems affect both buyers and vendors. Users may witness money loss due to vendors misbehavior (e.g. undelivered package after payment) and platforms exit scams (e.g. money theft from user's DNM deposit account). Cryptocurrencies, payment methods and vendor bond may form three mechanisms which can, if correctly implemented and used, mitigate the problems related to moral hazard.

Cryptocurrencies Cryptocurrencies are digital coins whose exchange does not need a trusted third party. Instead, cryptographic algorithms are used to verify and approve transactions. Some of the main features cryptocurrencies may provide are crucial for darknet markets users. For instance, Bitcoin can assure a certain level of anonymity, while Monero has been designed to be unlikely traceable, therefore enforcing privacy while keeping the overall system still anonymous to a certain extent.

Direct pay The most straightforward payment method is called Direct pay (DP): money is sent to the vendor immediately after she/he accepts the order. Moral hazard has a big impact when using this method: in case of disputes, support has no way to verify and check any form of scam.

Finalize early (FE) Very similar to the DP method. Money is sent to the vendor immediately after she/he labels the order with "shipped". This option is advised only when trading with trusted vendors, to minimize the risk of being scammed.

Escrow Most markets offers a traditional centralized escrow system, where money of the buyer for a particular purchase is collected and released to the vendor only when the buyer finalizes the purchase (i.e. the order has been delivered). In case of disputes, market's administrators will judge the situation and may refund the scammed party accordingly.

Multi-signature Most markets implements a 2-out-of-3 multisignature transaction scheme, where 2 out of 3 parties must approve a transaction to enable it. In this way none of all the involved parties can access and steal money alone. Platform or vendor scam are, therefore, less likely to happen.
The process consists of creating a multisig bitcoin address which is signed with 3 bitcoin public keys (one for each of the involved parties). Then the buyer sends the purchase amount to a market generated address. After finalizing, market gives its bitcoin private key to the vendor, which can unlock and retrieve the money. If order is canceled, then buyer gets the market bitcoin private key and the money is sent back to his/her e-wallet.

Vendor application In order to become a vendor on a marketplace, usually users have to go through an application process which consists of paying a one-time fee, known as vendor bond, or showing proof of previous trading history on other markets (mainly through PGP key verification), avoiding to pay any fee. In some cases the fee is refundable. For instance when vendor reaches 100 sales or after closing the account. Since applications for free require references to previous activity as a vendor, minimum effort scammers are not likely to join a market, unless they pay the bond, which however it is quite affordable is some cases. CGMC vendor application process is different from other markets (requirements, promotion, community comments) and seems to be the most difficult to complete, thus making this market less prone to the presence of several scammers. In general, vendor bond may be considered as a *weak signal* of moral hazard countermeasure, since it represents a commitment from the seller towards the platform.

4.2.2 Mechanisms addressing adverse selection

Adverse selection problem mainly affects buyers (e.g. when choosing a product based on a "non-direct" knowledge). However, it is also a concern of vendors (e.g. they are interested in having orders and disputed information about their buyers). Cryptocurrencies, payment methods and vendor bond may form three mechanisms which can, if correctly implemented and used, mitigate the problems related to moral hazard.

Phishing attacks Given that illicit hidden services are unlikely to SSL over Tor, usually it is difficult to assess the trustworthiness of a link. Phishing is one of the easiest way to obtain user credentials, by tricking the user into accessing a malicious website, that resembles the original one with aim, for example, of stealing credentials. Therefore several PGP signed mirror links are provided, in order to mitigate the risk of phishing for users. Moreover mirrors are useful whenever the main link is down for any reason (DoS or maintenance).

Encrypted messages: Pretty Good Privacy (PGP) Massages exchanged over the platform need to be sent in a secure manner. In fact, shipping addresses are exchanged between buyers and

vendors. Sending them in clear is a bad practice, since the market server can be under control or seized, leaking all the information which can put users at risk. Therefore using PGP (Pretty Good Privacy) encryption techniques may assure a better lever of confidentiality of the messages exchanged. Moreover through the use of public key cryptography, it is possible to create digital signatures to prove the authenticity of a particular actor. The principle is however straightforward. A buyer can use the vendors public key to encrypt a message. The vendor then uses his/her own private key to decrypt the message. Public key can be shared with any entity which can send encrypted messages to the vendor, who is the only one able to decrypt them through the secret private key.

Level system Some markets provide level system for vendors, which assure more information to the potential buyer. Points to acquire levels and status are earned by performing some particular activities (e.g. successfully completed order, positive feedback received) or can be lost by misbehaving (e.g. lost dispute).

Buyers information From both buyers and vendors perspectives, being able to check and trust each other information is a key point for quality trading. Usually reviews about vendors and products are always available, while it is less common to be provided with statistics about buyers reputations, orders, disputes and reliability. Vendors' concern is to avoid to sell illegal products to LE undercover agents, thus starting trading activities with trustworthy buyers could represent an incentive to remain in the market.

Partnership marketing Partnership marketing is a form of collaboration between two or more entities to achieve some business goals. It is only employed by 2 DNMs and only in Tier 1. Mainly used for quality control on products (mostly drugs), this service is meant to achieve harm reduction and it also helps reducing adverse selection problems. Moreover it refines vendors reputation.

Quest rewards Similar to the level system, but extended to every user (not only vendors), is the quest reward system. Only implemented on WallStreet Market, it gives badges and new status to members who perform certain actions:

- Award for using Multisig 5 times.
- Award for having a total of 100 different prices at the same time.
- Award for having 15 active offers listed on the market at the same time

4.2.3 Other mechanisms

CAPTCHAs and availability Mandatory login and CAPTCHA problem solving are needed before accessing the inner links of any platform. Hidden services on Tor have intrinsically scalability and traffic load limitations, due to the underlying technology employed. Moreover denial of service (DoS) attacks are very likely to happen resulting in the unavailability of the platform, with consequent loss of money for users and administrators. Using CAPTCHAs mitigates the problems derived from intensive bot crawling and the possible risk of DoS attacks.

Affiliate marketing Affiliate programs are a form of performance-based marketing where users can earn money by directing other users to the platform through the use of referral links. When Alice registers to the market using the referral link provided to her by Bob, there is a bonus for Bob. In addition profits are made on the commissions fee of the recruited buyers completed orders. Profits vary linearly among tiers:

- Tier 1: 20-45%
- Tier 2: 20-25%
- Tier 3: 10-20%

Chapter 5

Quantitative evaluation of market setups

In this section the results of our analysis on data collected from three selected Darknet Markets are discussed. This analysis is not meant to provide a full quantitative picture of the underground economy, but rather to provide quantitative insights to the operations of the considered platforms, where possible. By scraping the whole set of vendors profiles and feedback present on three selected platforms, we gathered information about the vendor names, their PGP keyID, the visible sales made and the correspondent feedback, the price of each reviewed sale, the possibility of receiving Finalize Early payments, and finally the dates in which sellers joined a market. Our analysis shows that distributions of revenues per sale generated by vendors FE-enabled and vendors FE-forbidden are similar and the revenues per sale aspect does not seem to be influenced by a durable activity on the market (there is no evidence of a clear mechanisms where *lack of trust is not taxed*). Successful vendors do not make large revenues per sale, instead they seem to rely on the amount of trades made.

Unique vendors A first look at the dataset reveals that among the three selected markets (Dream Market, Berlusconi Market and Olympus Market) there are 1941 vendors, reduced to 1769 when considering only unique PGP public keys. Considering that Dream Market alone hosts 1639 unique vendors, it becomes clear that most of the sellers are active on that platform and make use of one key for each identity in most of the cases. In fact the are only few vendors that associated the same key to different usernames. Berlusconi Market and Olympus Market have 116 and 155 unique active sellers.

Sales and revenues The total number of visible sales is 312471. The total amount of generated revenues is estimated to be around 32.6 millions EUR (1 BTC = 7000 EUR[1]), thus showing an average revenue per sale of about 105 EUR.

Dream Market generates around 30 million EUR, being the most populated and active platform. It makes available only at most 300 feedback for each vendor. In some cases 300 sales may be

[1] we considered an average value to provide a first rough estimation of platforms relative size. A quantification of economic transactions and value of platforms is outside the scope of this work.

market	vendor	unique	visible sales	revenue [EUR]	FE-allowed	FE-forbidden
All	1941	1769	312 471	32 658 085	722	1211
Dream Market	1670	1639	306 816	30 294 198	628	1034
Berlusconi Market	116	116	3764	2 186 939	39	77
Olympus Market	155	155	1891	176 948	55	100

Table 5.1: Statistics of the scraped platforms

made in few hours, while in others it may take several days. The largest timespan consists of 628 days, while the smallest is of 1 day, with an average timespan of 92 days.

Differently from the case of Dream Market, where only at most the last 300 feedback for each vendor are available, Berlusconi Market reports the entire sales and feedback history. Hence until June 2018 only 116 vendors are generating sales on this platform. The total amount of generated revenues is estimated to be around 2.2 millions EUR. The total number of visible sales is 3764, with an average of 32 sales per vendor. However the distribution is unbalanced, since only few vendors are responsible for the most of the generated revenues on the market. In fact, the top 2 successful vendors cover almost the 65% of the overall market volume. A second snapshot of Berlusconi Market (taken at the end of June) reveals that in one month the overall number of unique sellers increased of 10 units and the overall revenues are also a little larger, estimated to be around 2.5 millions EUR.

On Olympus Market from January 2018 till June 2018 (operating time of the market) the total amount of generated revenues made by 155 unique sellers (with 1891 sales) is estimated to be around 176000 EUR, thus showing an average revenue per sale of about 95 EUR. Olympus Market is a very concentrated market. platform. In fact 10 vendors make around the 50% of the total revenues on the platform.

Figure 5.1 shows the distributions of the revenues per sale in each market. On the x-axis the revenue per sale are represented, while on the y-axis their frequency is shown. The results suggests no evidence to support different behaviors among the platforms. Apart from few cases of very profitable sellers, the general trend is very similar. In fact, only 25 vendors (i.e. only the 1% of the total) generates revenues per sale above 1000 EUR, while remaining 99% of vendors generate revenues per sale around 100 EUR on average. The set of 20 vendors that generates the largest revenues per sale is reported in Table 5.2. Those vendors show a different behavior and represent the outliers on the graph. The two most profitable vendors (rows 10 and 17), respectively on Dream Market and on Berlusconi Market, are part of this set.

Finalize Early method After analyzing vendors' profile webpage we concluded that about 2 over 3 vendors are not allowed to receive payments through the Finalize Early method. In fact, vendors that are FE-allowed are 722, 1211 sellers are FE-forbidden and for 8 sellers there is no information availble on their FE status.

Figure 5.2 shows the distributions of vendors based on their join date (horizontal axis) and average revenue per sale (vertical axis with logarithmic scale); black dots indicate FE-enabled vendors, while red dots indicate FE-forbidden vendors. The result seems to suggest no particular advantage for older vendors on the market compared to the newest ones, in terms of revenues per sale. Arguably the market join date does not seem to represent a variable which can affect

the profits of users. In other words, presumably revenues are independent from the timespan a vendor has been present on the market. In addition there is no evidence for a significant difference among the revenues per sale generated by vendors FE-enabled and vendors FE-forbidden. Figure 5.3 shows the distributions of vendors based on their join date (horizontal axis) and their total revenues (i.e. volume) (vertical axis with linear scale). Here we can see the few outliers with high profits whose trend is different from the most of remaining sellers. Table 5.2 shows the top 20 vendors for revenues generated. We can see that most profitable vendors share a revenue per sale amount around or lower than 1000 EUR. The revenues per sale aspect, then, does not seem to be correlated to a durable activity on the market. Instead, most successful vendors are those who make lots of trades and receive lots of orders, and do not show large revenues per sale. Even with a long presence in the market and a high reputation, successful vendors seem to rely on quantity of orders during the time rather than the price of each sale.
Table 5.1 summarize the data we reported. We conclude that Dream Market is a highly active darknet market, despite its scarce sense of security and few features available. The largest market share is of 1.33%, with an average of 0.06%, suggesting there are several competing vendors on this platform. Here with market share we intend the ratio between the share of a vendor and the total amount, thus only referring to a certain timespan and number of feedback. Most of vendors are FE-forbidden, but this does not seem to affect the overall revenues after all. At the time of writing Dream Market represent the most populated and apparently successful (in terms of profit the administrators) operating market. We argue that for the time being it still represent the biggest source of listings and vendors to new and old buyers among the most popular darknet markets operating over Tor network.

market	vendor	keyID	visible sales	revenue [EUR]	revenue/sale [EUR]	market share %	FE	join date
berl	g00d00	0x820AD992	685	1114875	1628	50.98	Yes	2017-7-25
dm	dank_green3	0x001332F6	300	402500	1342	1.33	No	2017-7-12
dm	TheXanaxPlug	0xEFBC76A7	300	312300	1041	1.03	Yes	2016-3-31
berl	Barcelona	0xA2194D1E	386	299958	777	13.72	No	2017-8-27
dm	budds-all-day	0x137878A2	300	277115	924	0.91	Yes	2018-2-24
dm	PlatinovWarehouse	0x7E2129DB	300	277115	924	0.91	No	2018-4-23
dm	PoundPound	0x1F31117B	300	266255.2	888	0.88	No	2017-8-31
dm	milkman11new	0xDF67D8BB	300	244305	814	0.81	Yes	2017-10-14
dm	PasitheasTemp	0x7B518A58	145	220850	1523	0.73	No	2018-4-21
dm	WashingCannabisCo	0x5A807F27	265	207100	782	0.68	No	2016-12-13
dm	BartardCo.	0xC787C9F5	300	185643	619	0.61	Yes	2017-11-4
dm	CHEST	0xBB9CF85E	293	152500	520	0.5	Yes	2015-11-1
dm	RebelAllianceRX	0x81307B60	300	138520	462	0.46	No	2017-11-20
dm	MendocinoGreeno	0x9A70B6BF	300	138350	461	0.46	No	2015-12-19
dm	YoungAmsterdam	0xED3BA65C	272	137410	505	0.45	No	2016-5-7
dm	xangod	0x3BB520D1	300	130205	434	0.43	No	2018-4-3
dm	Surefour	0x29B026AE	218	128665	590	0.42	No	2017-11-11
dm	HonestCocaine	0xE47840A8	159	125100	787	0.41	Yes	2016-9-17
dm	ASAPmolly	0xE94AE663	141	123230	874	0.41	Yes	2015-12-5
dm	lyso	0x1341CAF1	300	123193.5	411	0.41	Yes	2015-11-8

Table 5.2: Top 20 vendors based on total revenues

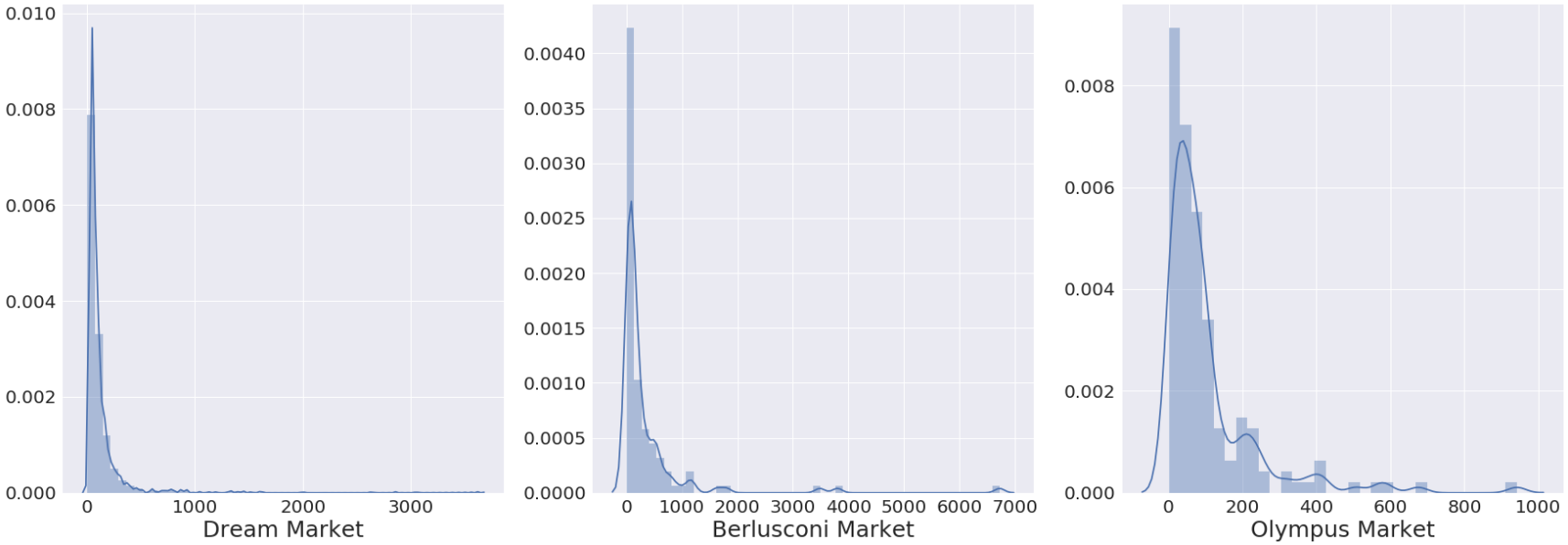

Figure 5.1: Distribution of revenues per sale of vendors on each platform

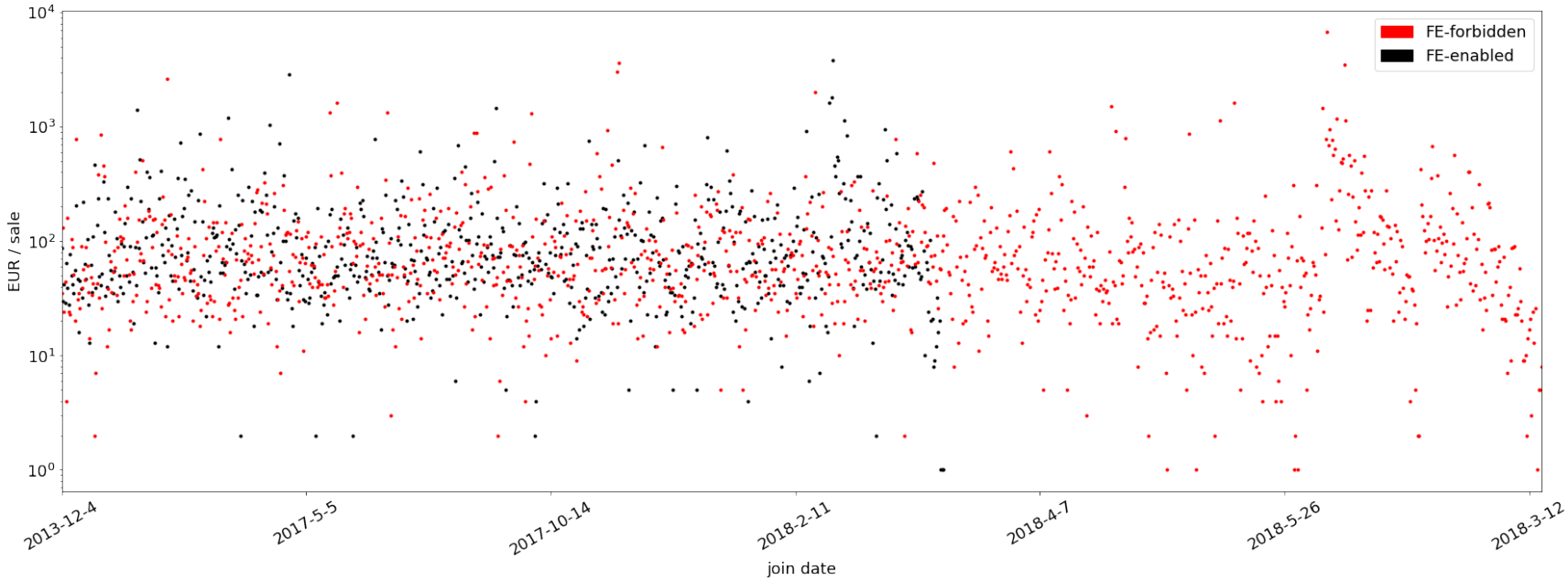

Figure 5.2: Distribution of vendors based on their join date and average revenue per sale (logarithmic scale)

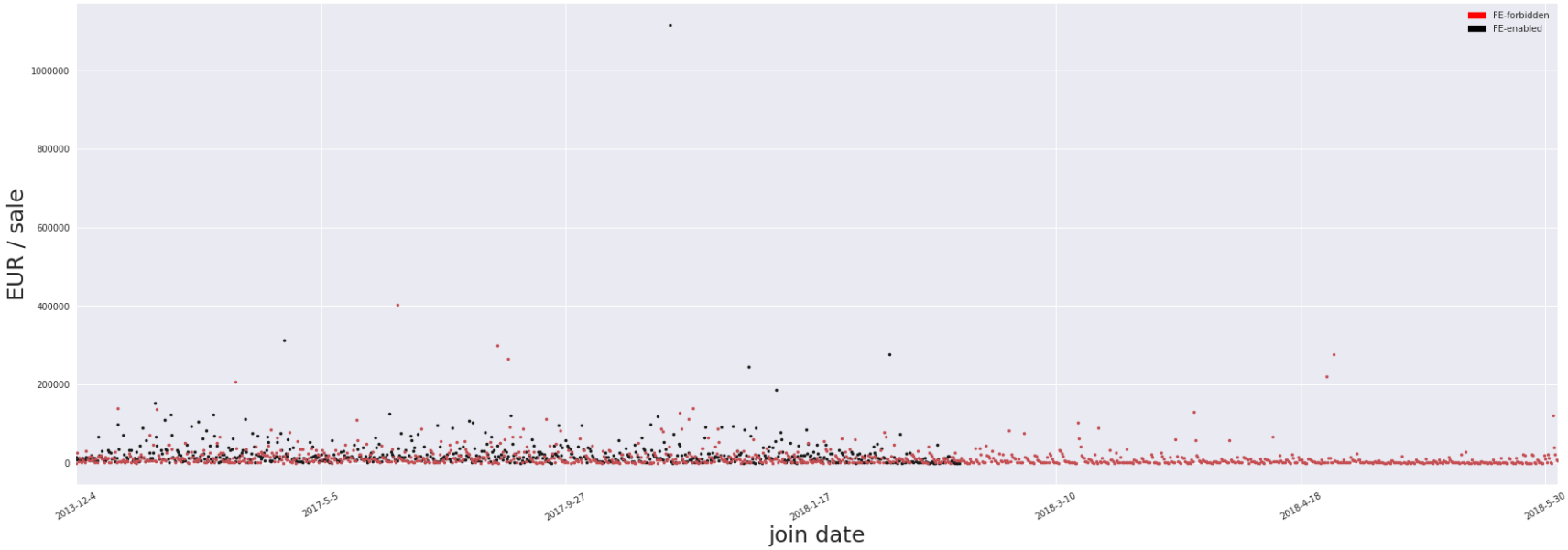

Figure 5.3: Distribution of vendors based on their join date and revenues generated (linear scale)

Chapter 6

Discussion and Conclusions

This section contains the results and lessons learned in this research project.

We explored the Darknet Markets ecosystem, focusing on the strategies that platforms adopt to differentiate themselves from the competition and the features which may drive users decisions, with the intent to relate those to the problems of moral hazard and adverse selection. We assessed vendors behaviors on three different markets in terms of generated revenues and timespan activity. We found that technology has created new ways of managing transactions and trades of illegal goods among parties, reducing the risk of being exposed to law enforcement investigations, street violence and harmful substances.

So far, the underground online ecosystem has been resilient to disruptions, take-overs and seizures by police. In fact, several platforms quickly emerge and overall revenues tend to increase over time. Reputation and regulation mechanisms have been considered as the key features for market liveness and reliability. Without them markets are going to collapse. However they are not sufficient to guarantee a safe and trustworthy environment to buyers and sellers, since also the platform plays an significant role in addressing users concerns (for instance, security of sensitive data and availability of services). The act of purchasing is the moment of maximum exposure to risk. Illicit goods are shipped and unregulated transactions are carried on, thus users may become subject to law enforcement investigations or scammed by vendors (or platforms). Therefore the focus is all on own operational security and payment methods.

Security, privacy and safety of transactions are main concerns among DNMs users. Reducing information asymmetry by employing security features and providing reliable information both to buyer and users, ideally platforms can guarantee the most suitable environment for illicit online trading. Platforms may or not guarantee a satisfactory measure against moral hazard problems. For instance, they can try to mitigate it through the use of multisignature payment schemes instead of relying of classic escrow systems, which put the money held by the platform (and belonging to users) at risk. Darknet markets can also mitigate the adverse selection problems with several means. They can set up an environment where, not only reputation mechanisms are enforced, but also more information is available. For instance by making the approval of a vendor subjective to other users decision, or providing a quality control partnership for harm reduction. In this way buyers can better assess the type of dealer they are facing and the quality of goods he/she sells.

Recalling the research question presented in Section 1.3, we give the results of our study.

Which are the strategies and mechanisms that minimize the uncertainty derived by law enforcement operations and scammers in the market?

We found inconclusive evidence to support an interest by Darknet market administrator to make the platform more appealing and secure for its users. On the most successful market, no multisignature system is in place, vendors cannot check buyers information, scammers are frequently reported, support is considered to be flawed and several security issues have been found, but never solved. However it represents one of the biggest sources of sellers for the darknet community. Therefore it is a platform with no real valid alternative to it in terms of volume and listings. It is a very competitive environment, with lots of vendors and a quite distributed market share among them. On the other hand smaller markets tend to be more concentrated, with very few vendors being profitable. It is worth mentioning the the most profitable vendor is active on both Dream Market and Berlusconi Market. However his/her total revenue on the former is only around 30000 EUR, while on the latter he/she has generated two orders of magnitude more revenues (in less than a year). Other emerging (or established for 1-2 years already) platforms are proposing different environment to their users where a sense of social community is enforced. The case of CGMC is very significant. It has very few vendors and it is specialized only on cannabis and derivatives. It has an highly active internal forums where vendors applications are reviewed and voted by the community (thus reducing the presence of scammers). So the key points are sense of community, shared information, active support and quality of vendors. However, there is currently insufficient evidence to conclude whether emerging markets are going to witness a significant growth in the coming future, despite their approach towards different business models than those used by established markets. Additional longitudinal studies will be required to give a final answer to this question.

We have also discussed how markets can be closed, users arrested and communities monitored. Uncertainty is not only among buyers and vendors, but it also affect platforms administrators. Markets do not seem to last very long (with the exception of Silk Road in the past and, currently, Dream Market). Other studies revealed how the underground activity continues even in presence of disruptions and seizures. Once the biggest markets is taken down, other platforms will gather users, according to mechanisms that so far are still unknown. Arguably administrators of small and medium markets may take actions to place themselves in the underground environment in such a way to become the next most successful platform. When looking at revenues and numbers of sellers, darknet markets ecosystem seems quite concentrated, with only a few highly successful vendors. Large volume platforms (such as Dream Market) do not offer any particular feature which may be fundamental for its growth, but still managed to become an active leader after the closure of Hansa and Alphabay which were the largest markets at the time. Arguably, assuring a functional system after the shock derived from law enforcement investigations which disrupted competition, seem to have been a successful strategy. In our research we have not found any evidence that contradicts the hypothesis of strategic positioning. However, additional studies are needed in order to assess the matter and give derive proper insights from larger observations.

Focusing on the competitive advantage among platforms we found that the actual big markets are no safer than other smaller and less popular DNMs. Instead, big markets do not seem to be very careful about security features and safer payment methods, while smaller and emerging markets are more customer-centric and security focused. Collected evidence do not seem to indicate which market is going to take the place of the actual biggest platform. A possible pointer for market success might be specializing into a particular category of products.

6.1 Limitations

Our study has some limitations. First, qualitative investigation cannot provide conclusive evidence and should only be interpreted as a first characterization of underground markets. Second, our quantitative data collection covers only three markets, since heavily reported scamming website have been excluded, but still may constitute an important source of information. In fact, given the illicit nature of the context and the anonymizing services in places, deciding whether a platform is reliable or not is far from being an easy task. Thus there are few markets we excluded (such as Valhalla and Silk Road 3.1), because, even if apparently quite populated and active, they have been reported to scam their users or being LE honeypot that attract and monitor orders and shipping. Nevertheless, some highly successful sellers we found on the chosen markets seem to be present also on those excluded. Hence a deeper investigation is needed to assess the authenticity of those entities, since sometimes users may copy usernames on other platforms. For our quantitative analysis we only considered three markets for other two reasons: first, not all of the platforms make the amount of money involved in each purchase available; second, some markets (such as Wall Street Market and CGMC) are difficult to scrape since they seem to implement a good defense against automated crawlers and bots. Therefore, scripts should be improved to scrape data from a wider range of different platforms. Information regarding shipping information and statistics (and changes over time) about the product listings also needs to be analyzed in order to derive a more detailed picture of the underground ecosystem.

Bibliography

[1] https://www.investing.com/crypto/currencies. [Online; accessed 13-08-2018]. 8

[2] Bitcoin 'exit scam': deep-web market operators disappear with 12mln USD. https://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars. [Online; accessed 14-08-2018]. 11

[3] Dark Web Users Suspect "Dream Market" Has Also Been Backdoored by Feds. https://thehackernews.com/2017/07/dream-market-darkweb.html. [Online; accessed 02-04-2018]. 24

[4] Dream Market: A Hotbed of Scammers. https://darkwebnews.com/darkwebmarkets/dream-market/dream-market-a-hotbed-of-scammers/. [Online; accessed 07-06-2018]. 24

[5] Feds Bust 'Farmer's Market' For Online Drugs. https://www.darkreading.com/attacks-and-breaches/feds-bust-farmers-market-for-online-drugs/d/d-id/1103901. [Online; accessed 13-08-2018]. 7

[6] Feds bust Farmers Market, an online illegal drug ring hidden by TOR. https://www.digitaltrends.com/web/feds-bust-farmers-market-an-online-illegal-drug-ring-hidden-by-tor/. [Online; accessed 13-08-2018]. 7

[7] I Used the Dark Net's First Search Engine to Look for Drugs. https://motherboard.vice.com/en_us/article/z4m4ma/i-let-grams-guide-me-through-the-dark-nets-illegal-bazaars. [Online; accessed 25-02-2018]. 14

[8] Italian Man Busted After Returning to a Burned Drop. https://www.deepdotweb.com/2018/08/09/italian-man-busted-after-returning-to-a-burned-drop/. [Online; accessed 09-08-2018]. 3

[9] OPERATION BAYONET: INSIDE THE STING THAT HIJACKED AN ENTIRE DARK WEB DRUG MARKET . https://www.wired.com/story/hansa-dutch-police-sting-operation/. [Online; accessed 3-08-2018]. 3

[10] Ransomware doesn't sell itself: Marketing malware on the darknet. https://blog.avast.com/ransomware-doesnt-sell-itself-marketing-malware-on-the-darknet. [Online; accessed 25-02-2018]. 14

[11] Romanian Arrested After Four Package Interceptions. https://www.deepdotweb.com/2018/03/31/romanian-arrested-four-package-interceptions/. [Online; accessed 31-03-2018]. 3

[12] The Darknet Search Engine Grams is Shutting Down. https://www.deepdotweb.com/2017/12/15/darknet-search-engine-grams-shutting/. [Online; accessed 25-02-2018]. 14

[13] TOR DNM-RELATED ARRESTS, 2011-2015. https://www.gwern.net/DNM-arrests. [Online; accessed 01-06-2018]. 3

[14] Wall Street DNM IP exposed. https://twitter.com/x0rz/status/921016966596440066. [Online; accessed 08-02-2018]. 27

[15] Wall Street Market's IP address is exposed. https://www.reddit.com/r/onions/comments/77jfd1/wall_street_markets_ip_address_is_exposed/. [Online; accessed 08-02-2018]. 27

[16] Alois Afilipoaie and Patrick Shortis. From Dealer to Doorstep How Drugs Are Sold On the Dark Net. *Global Drug Policy Observatory*, 2015. 2

[17] Alois Afilipoaie and Patrick Shortis. Operation Onymous: International law enforcement agencies target the Dark Net in November 2014. *Global Drug Policy Observatory*, 2015. 8

[18] Alois Afilipoaie and Patrick Shortis. The Booming Market of Alternative Cryptocurrencies. *Global Drug Policy Observatory*, 2015. 8

[19] Alois Afilipoaie and Patrick Shortis. The Growing Industry of Darknet Marketing. *Global Drug Policy Observatory*, 2015. 14

[20] George A. Akerlof. The market for "lemons": Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84(3):488–500, 1970. 10

[21] L. Allodi, M. Corradin, and F. Massacci. Then and Now: On the Maturity of the Cybercrime Markets The Lesson That Black-Hat Marketeers Learned. *IEEE Transactions on Emerging Topics in Computing*, 4(1):35–46, Jan 2016. 13

[22] Angus Bancroft and Peter Scott Reid. Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. *International Journal of Drug Policy*, 35:42 – 49, 2016. Drug Cryptomarkets. 1

[23] Monica J. Barratt, Jason A. Ferris, and Adam R. Winstock. Safer scoring? cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy*, 35:24 – 31, 2016. Drug Cryptomarkets. 1

[24] V. Bhaskar, Robin Linacre, and Stephen Machin. The Economic Functioning of Online Drugs Markets. CEP Discussion Papers dp1490, Centre for Economic Performance, LSE, July 2017. 11, 12

[25] Joe Van Buskirk, Raimondo Bruno, Timothy Dobbins, Courtney Breen, Lucinda Burns, Sundresan Naicker, and Amanda Roxburgh. The recovery of online drug markets following law enforcement and other disruptions. *Drug and Alcohol Dependence*, 173:159 – 162, 2017. 3, 8

[26] Alvaro Cardenas, Svetlana Radosavac, Jens Grossklags, John Chuang, and Chris Hoofnagle. An Economic Map of Cybercrime. 08 2009. 12

[27] Nicolas Christin. Traveling the silk road: A measurement analysis of a large anonymous online marketplace. *CoRR*, abs/1207.7139, 2012. 8

[28] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, SSYM'04, pages 21–21, Berkeley, CA, USA, 2004. USENIX Association. 7

[29] Martin Dittus, Joss Wright, and Mark Graham. Platform Criminalism: The 'Last-Mile' Geography of the Darknet Market Supply Chain. *CoRR*, abs/1712.10068, 2017. 9

[30] EMCDDA and Europol. Drugs and the darknet: perspectives for enforcement, research and policy. Joint publications, 2017. 3, 9

[31] Steven Goldfeder, Joseph Bonneau, Rosario Gennaro, and Arvind Narayanan. Escrow protocols for cryptocurrencies: How to buy physical goods using bitcoin. In *Financial Cryptography*, 2017. 11

[32] ROBERT AUGUSTUS HARDY and JULIA R. NORGAARD. Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. *Journal of Institutional Economics*, 12(3):515539, 2016. 13

[33] Thomas J. Holt, Olga Smirnova, and Alice Hutchings. Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, 2(2):137–145, 2016. 13

[34] N. Janetos and J. Tilly. Reputation Dynamics in a Market for Illicit Drugs. *ArXiv e-prints*, March 2017. 8

[35] Kruithof Kristy, Aldridge Judith, Dcary Htu David, Sim Megan, Dujso Elma, and Hoorens Stijn. Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands. RAND Corporation, 2016. 2

[36] Anita Lavorgna. Organised crime goes online: realities and challenges. *Journal of Money Laundering Control*, 18(2):153–168, 2015. 14

[37] James Martin. Lost on the silk road: Online drug distribution and the cryptomarket. *Criminology & Criminal Justice*, 14(3):351–367, 2014. 8

[38] Daniel Meja, Pascual Restrepo, and Sandra V. Rozo. On the Effects of Enforcement on Illegal Markets : Evidence from a Quasi-experiment in Colombia. 2015. 7

[39] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf. 7

[40] P. REUTER and J. P. CAULKINS. Illegal lemons: price dispersion in cocaine and heroin markets. In *Bulletin on Narcotics*, volume LVI, chapter 6, pages 141–165. 2004. 1, 3, 10, 11

[41] Kyle Soska and Nicolas Christin. Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In *Proceedings of the 24th USENIX Conference on Security Symposium*, SEC'15, pages 33–48, Berkeley, CA, USA, 2015. USENIX Association. 8, 9