Boarding a sinking ship

trust mechanisms in the underground in the face of high market platform volatility

Wouters, R.

Award date:
2019

Technische Universiteit Eindhoven University of Technology
Department of Mathematics and Computer Science
Security Group

Boarding a Sinking Ship: Trust Mechanisms in the Underground in the Face of High Market Platform Volatility

Masters' Thesis

René Wouters

Supervisor:
Dr. Luca Allodi

Assessment Committee:
Dr. Luca Allodi
Dr. Benne de Weger
Dr. Nicola Zannone
Dr. Bert Sadowski

Eindhoven, September 2019

Abstract

Background The majority of current online illegal drug trading takes place on Darknet market platforms on the popular anonymity network Tor. Due to their illegal nature, these market platforms frequently get shut down. Due to this, users have to continuously change communities, and the ability to create trust in such a community in the face of frequent interruptions is difficult. This thesis aims to research which trust-building mechanisms, classified here into organic trust-building mechanisms and technological trust-building mechanisms, are valued most highly by market platform users.
Methodology Quantitative results relating to user preference between the various kinds of trust-building mechanisms were gained through a survey distributed to Darknet community users and Darknet market vendors through direct messaging. General statistical information concerning Darknet market platforms was obtained through scraping these market platforms and categorizing the scraped data with an LDA (latent Dirichlet allocation) model.
Results Both qualitative and quantitative results gained from the survey show that a majority of the survey respondents noted they preferred organic trust-building mechanisms over technological trust-building mechanisms. The respondents also indicated that they did not place trust in the market platforms themselves, because they believed that an individual market platform's existence was temporary. Believing it would either be taken down by law enforcement or by an exit scam performed by the market platform administrators.
Conclusion Users greatly preferred trust-building mechanisms that allow users to create bonds of trust between each other. Market platforms administrators are therefore best served by creating tools that allow such bonds to be created more easily. On the other hand, the trust users placed in Darknet market platforms was generally low, as the presence of these market platforms was seen as short-lived. Therefore, Administrators are also best served by creating a market platform infrastructure which removes their ability to commit and exit scam as much as possible.

Contents

Chapter 1

Introduction

Online marketplaces have become a growing avenue used for the buying and selling of illegal goods in the past decade. As regular online traffic can be tracked remotely by law enforcement agencies or anyone with enough technical capabilities, the online drug market has mostly migrated to the Darknet, a colloquial name for the mass of anonymity networks that are not accessible by the general public through "standard" Internet browsing software. Among these anonymous networks, the Tor network is perhaps the most popular one. Because of the increased anonymity provided by the Tor network, it has become the primary place used for selling illegal drugs online. To facilitate this trade, several Darknet marketplaces have cropped up over the years.

These marketplaces are similar in function to well-known legal marketplaces such as eBay or Marktplaats, but due to their inherently illegal nature, these marketplaces are frequently taken down by law enforcement agencies. While a lot of research has been performed on darknet markets in general[5][40][29], less research has been done on other aspects of Darknet user behaviour.

On legal marketplaces, users can appeal transactions if a user has been scammed because many laws are in place to protect both vendors and buyers from such actions. Since no legal protections exist in Darknet markets due to their illegal and anonymous nature, establishing trust between buyer and vendor becomes even more critical. The building of such trust can be aided by several mechanisms, both created by Darknet administrators, and by the market platform users themselves. Furthermore, when a market platform takedown takes place, the community of that platform gets broken up as users move to other market platforms.

The means with which these users establish trust between each other in the face of these above complications is not very well researched, nor are the effect on repeated market platform takedowns on community trust and behaviour well understood. Some research was done to conclude that some users completely removed their identity and bonds of trust they had with the community[42], but individual market user behaviour is poorly researched. Furthermore, the majority of these markets get shut down by the authorities or by the administrators themselves by what is called an exit scam. Users are aware of this, but as no other avenues to purchase drugs on Tor exist, they have no other choice. Hence the title "boarding a sinking ship", as both the vendors and buyers realize that the market platforms they operate on are temporary, but join these platforms regardless.

In the face of the temporary nature of these market platforms, buyers and vendors still need mechanisms to create trust among each other in order to successfully complete transaction. This thesis aims to research the various trust-building mechanisms that are available on various market platforms and research which types of trust-building mechanisms are valued most highly by market platform users. To accomplish this, a survey was created to question Darknet market users which trust-building mechanisms they found to be most valuable, and whether the frequent darknet market shutdowns have affected their behaviour or general Darknet market usage.

Research Question:

In order to discover what these trust-building mechanisms used in Darknet markets are, the following research question has been formulated:

RQ: What mechanisms underlie the trust-building dynamics in underground market platforms?

To answer this question, a means to contact and question the Darknet market community is required. In order to achieve this, a survey was created which was used to ask both qualitative and quantitative questions to the Darknet community regarding both trust-building mechanisms and their behaviour in the face of frequent market platform takedowns.

Furthermore, in order to gather more general statistics about Darknet market platforms, a statistical analysis of various Darknet market platforms was performed. In order to categorize this data further, an LDA model was developed which categorized the vendor profiles gained from this statistical analysis. This information was then used to create a representative sample of each market platform vendor's population. The vendors in this sample were then sent the survey in order to keep the survey respondent pool as statistically representative as possible.

Chapter 2

Background

2.1 The Darknet

To understand what the Darknet is, it is best to define the term first. The Darknet, or dark web, is not actually a separate network from the traditional World Wide Web, or Internet. It is simply a virtual network of websites that cannot be reached using conventional web browsers such as Microsoft Edge or Chrome. The Tor network is also not indexed by search indexers, such as Google or Bing. Therefore, if one wanted to access the Darknet, specialized software would be required in order to do so. Note that the Darknet is different from the deep web, which, while still part of the normal Internet, cannot be indexed by normal search engines either. The deep web encompasses many different networks such as corporate networks, library networks and other secure databases[7].

The term Darknet was first coined in the 1970s to refer to a network that was separate from ARPANET, the network that would eventually grow into the worldwide information network known as the Internet. These Darknets could receive information from ARPANET, but these Darknets would not show up on ARPANET server lists or respond to pings. Originally, such networks were created due to security restrictions, but other networks created for various other reasons soon started to appear.

Due to its nature, the Darknet has a host of useful properties that are attractive for various reasons. Most applications that connect to the Darknet also try and obfuscate the connection, thereby allowing the user to remain anonymous. Tor, for instance, automatically encrypts and routes any traffic via a set of random relays in the Tor network before the data reaches its destination. The increased privacy guaranteed by the Tor protocol is therefore useful in many different applications.

In modern times, the Darknet is used by a large number of people for a variety of applications. Whistleblowers use the Darknet to anonymously distribute information, journalists and NGOs use it to securely receive information and dissident and activist groups utilize the Darknet in order to plan their activities [35]. A further major aspect of the Darknet, and one that will be further discussed in this thesis is the proliferation of illicit activities such as the sale of illegal drugs and weapons, the hiring of services such as assassinations or DDoS attacks, copyright infringement, and distributing illegal material such as child pornography.

Due to these activities, the Darknet faces regularly attempted takedowns by various national law enforcement agencies. Darknet drug markets regularly get taken down by authorities because they sell illegal drugs. Some notorious examples of this are the takedown of the AlphaBay [37] and Hansa [23] markets.

Some governments block access to the Darknet as they cannot properly control and monitor what gets posted and stored on such networks, and therefore believe that restricting access to such networks will serve the public good. Nations such as Russia [12], China [44], and Iran [21] have all tried to block access to the Darknet and Virtual Private Networks (VPNs) in general.

2.2 The Tor network and its hidden services

Tor is currently the most well-known method of accessing the Darknet. The Tor network allows anonymous users to deploy so-called "hidden services". A hidden service, or onion service, is the equivalent of what would be a web server on the normal Internet. Hosting a hidden service on the Tor network can therefore be considered equivalent to hosting a web page on the regular Internet. A hidden service is hosted on a server just like a website is, but is instead configured to receive connections through the Tor network. Instead of using an IP address to identify itself, it uses an onion address for identification, accessible through the Tor browser. This onion address is associated with the public key of the hidden service, which is generated together with the private key on the hosting server when the service is created.

The process of creating a hidden service and having a client connect to it proceeds as follows:

1. Create a hidden service and randomly pick 3 Tor nodes as introduction points
2. Advertise your hidden service on a database
3. If a client wishes to connect to the service, they choose a random Tor node as a rendezvous point and downloads the hidden service summary from the database
4. The client sends an encrypted message to the hidden service containing the rendezvous point and a one-time secret
5. The hidden service connects to the rendezvous point and shares the one-time secret
6. The connection is established and client and hidden service can now communicate anonymously through the rendezvous point

When a hidden service is created, it first connects to a number of Tor relays, machines that encrypt and route Tor traffic, and designates those relays as introduction points. The service then creates an onion service descriptor from a summary of the introduction points and public key and signs this with its private key. The service then proceeds to send this descriptor to a distributed hash table.

For this reason, onion addresses are generally a random string of numbers instead of a human-readable name. http://4ntfw4clmfemmvtn.onion is the onion address for the hidden service which hosted the survey created for this thesis, for instance.

If a client knows about the onion address and wishes to connect to it, first the client's Tor browser will download its descriptor from the distributed hash table. It will then select a random Tor relay as the rendezvous point. When this rendezvous point is ready, the client creates an *introduce* message which includes the address of the rendezvous point and a one-time secret, encrypts this with the hidden service's public key, and sends this message to one of the introduction points, requesting it be sent through to the hidden service.

Finally, the hidden service creates a Tor circuit to the rendezvous point and sends the decrypted one-time secret to it. When the rendezvous point receives the one-time secret, it notifies the client that a connection is established and the client and hidden service will then communicate anonymously through the rendezvous point.

2.3 Darknet markets

Darknet markets, which are hosted on Tor hidden services, have emerged as a major avenue in the trade of illicit goods. Selling illicit material through online means has a long history. Indeed, the very first e-commerce transaction was a sale of an undisclosed amount of Cannabis made between a student at MIT and a student at Standford using the ARPANET network [9]. Over the decades, this practice has grown into a business worth hundreds of millions of US dollars annually. Figure 2.1, taken from [11], shows an overview of the various different types of drugs and services that can be purchased on cryptomarkets. As can be seen from the Figure, while drugs are the primary

goods on offer, items such as video games or accounts for various websites also account for a significant amount of total sales. Van Wegberg et al[41] further supports this, having found that some markets offer various other forms of commodities not limited to drugs, including Malware, accounts for various websites, and various pirated material just to name a few examples. The total revenue van Wegberg estimated from these sales in total amounted to more than 28 million dollars.

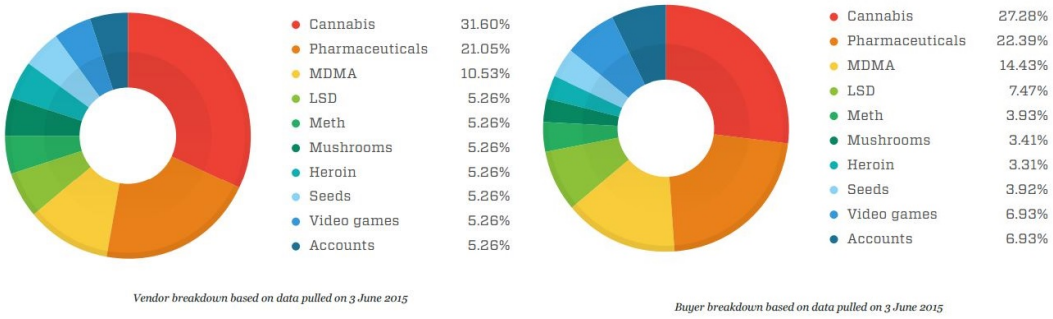

Figure 2.1: An overview of the distribution of sales in Darknet markets. Taken from [11]

While Darknet markets offer an avenue for dealing in illicit drugs, services or other illegal goods, a case can be made that such markets actually decrease the violence associated with illegal transactions.[6]

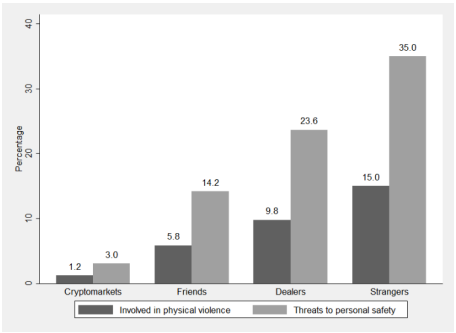

Figure 2.2: A comparison of physical violence between several illicit market types. Taken from [6].

Physical trade in drugs, for example, entails different risks for both vendors and buyers. Beyond the greater exposure to law enforcement agencies, the risk of physical violence is also present when making a sale in person. Figure 2.2 is taken from a study which surveyed the experience of cryptomarket users buying drugs and compares these experiences to their experiences when buying drugs from strangers or friends. As can be seen from the Figure, the risk of physical danger is around 8 times as low when using cryptomarkets compared to in-person dealers (1.2% versus 9.8%). A digital marketplace greatly lowers the risk of physical violence from the transaction, leading to fewer deaths due to the drug trade. Because these marketplaces also deliver internationally, buyers have more choices when purchasing drugs compared to the comparative monopoly of their local drug dealer who might not necessarily have the safest or highest quality product available.

Darknet markets also offer the opportunity to ship larger quantities of drugs wholesale for use by smaller-scale offline drug dealers themselves. Aldridge et al. reviewed revenues generated by the Silk Road marketplace in September 2013 and found that around 25% of the revenue generated by the platform came from sales deemed wholesale-level ($>$ 1000 US dollars in value)[5].

Top Market Platforms	**Vendor Shops**
Dream Market	Gammagoblin
Wall Street Market	The French Connection
Tochka	CharlieUK
Market Platforms	ToYouTeam
The Majestic Garden	The Church (joR)
CGMC	RechardSport
Berlusconi Market	DutchDrugz
Cannazon	
Discussion Forums (independent)	
Dread	
Darknet Avengers	
The HUB	

Table 2.1: An overview of the various markets and Darknet-based forums that are operational according to DeepDotWeb in February 2019 [1]

While originally the trades might have been performed on an ad-hoc or individual basis, many organized market platforms have cropped up to facilitate easier and more secure contact between prospective buyers and vendors. Various websites surrounding these markets have also cropped up. As can be seen from table 2.1 from the darknet news site DeepDotWeb a website dedicated to "all-things cryptomarket", there are several reported market platforms. This thesis will cover the major Darknet market platforms that were online at the time of the writing of this thesis, those being Empire Market, Berlusconi Market, Wall Street Market, Cryptonia Market, and Tochka Market. In the following sections, some of the major or influential darknet markets that are now defunct will be discussed in order to show the various ways that Darknet markets can get taken down.

2.4 A brief history of defunct market platforms

There are two main means through which a cryptomarket usually gets shut down, either through a takedown by law enforcement agencies or by what is called an exit scam. An exit scam occurs when the administrators of a cryptomarket empty a market platform's escrow accounts and leave the market to die. An exit scam can cause large amount of damage to the trust users have in the cryptomarket ecosystem in general. While law enforcement takedowns are expected due to the illegal nature of the platform, the threat of exit scams means that the market platforms themselves can no longer be trusted.

What follows is a rundown of only a few of the market platform failures reported to date. A more complete overview can be found in the 2017 Europol report on the Darknet market drug trade[20].

2.4.1 Silk Road: shut down by the authorities

Silk Road was launched by Ross Ulbricht under the name "Dread Pirate Roberts" in February 2011 [22]. The Silk Road can be seen as the first iteration of the type of markets that will be researched in this thesis. It was the first market platform that completely utilized Tor from the start and was also the first of its kind to exclusively use Bitcoin escrow for its transactions. Previous illegal drug markets, such as the Farmer's Market, which launched around 2006, was still using regular payment processors such as PayPal and Western Union, allowing law enforcement agencies to more easily trace payments and shutting the platform down. The Silk Road's use of Bitcoin, together with its use of the Darknet through Tor, set the tone that the majority of future market platforms would follow.

After the arrest of its creator, the original Silk Road shut down in October 2013 [27]. Several operators of the Silk Road attempted to restart the service under the name "Silk Road 2.0" on November 2013, but this was shut down by authorities as well in late 2014 [2]. There were also multiple further attempts to create markets capitalizing on the Silk Road brand, but none managed to stay online for long or gather a large amount of users. [38] [17]

2.4.2 AlphaBay and Hansa: infiltrated and shut down by the authorities

AlphaBay and Hansa were, at the time, the first and third largest market platforms respectively. Over ten time the size of the Silk Road at its height, AlphaBay had over 400,000 users and 369,000 listings and was trading around 600,000 to 800,000 US dollars every day [36]. However, lax security practices by its founder, Alexandre Cazes, allowed American law enforcement agencies to identify him in Thailand and issue a warrant for his arrest. After being arrested by the Thai authorities, Cazes committed suicide in his prison cell. After the American authorities announced the shutdown of the market, an exodus started by former AlphaBay users to other markets, and a large proportion of those users went to Hansa.

Unbeknownst to these users, however, Hansa was already under surveillance by Dutch authorities in collaboration with Interpol. Earlier in the year, the Dutch police managed to arrest the main operators of Hansa market and gained access to their login details. Instead of shutting the market down as was usual with such an operation, they decided to keep the market operational in order to gather as much information on the major vendors and buyers as possible. To do this, the police changed the Hansa codebase in various ways. The passwords were no longer hashed, but simply stored in plaintext, any pictures uploaded would now keep their metadata, allowing the police to find their location, and the encrypted communication between buyers and vendors was broken into, allowing the police to gather many user's real addresses. This investigation only became more effective when the number of new users increased by 800% after the shutdown of AlphaBay [23]. When the volume of transactions became too great for Europol to keep documented, Hansa was finally shut down as well. The information gathered during this investigation, termed operation Bayonet [23], was later used to arrest the largest buyers and vendors on Hansa and many more were issued warnings.

This operation lead to a great amount of chaos on the Darknet. Unlike previous shutdowns like Silk Road, where the users quickly migrated to other markets and continued their activities, these two shutdowns seemed to have had a larger effect than before, with many users either quitting their activities altogether, or creating entirely new identities. The volume of trade on such centralized markets seems to have also decreased, as the largest market currently online, Dream Market, seems to have not reached the volume of trade AlphaBay had even 3 years later.

2.4.3 Wall Street Market: exit scam followed by law enforcement takedown

Only launched in 2016, Wall Street Market is one of the newest market platforms on the Darknet. Perhaps due to its young age it attempts to be a more modern iteration of a Darknet marketplace. It is the only market discussed here that accepts Monero, something AlphaBay was known for shortly before it was shut down. Monero is a cryptocurrency based on the Cryptonote [3] protocol, which allows users to obscure the transaction trail by including chaff transactions called "mixins" to obscure the real transactions. Bitcoin does not offer this added anonimity since it explicitly shows the complete, unaltered transaction trail. This functionality allows Monero users to spend their currency with increased privacy[33]. It also offers multisig support, beyond all the "standard" features (review system, rating system).

In mid-April, users of Wall Street Market noticed that they could no longer withdraw money from the escrow wallets used by the market. Initially, the administrators told users that this was a temporary connection issue, and that the administrators had temporarily moved the funds to another wallet until the issue was resolved. Users were unimpressed with this explanation, and accused the administrators of perpetrating an exit scam[13]. The traffic generated by this event

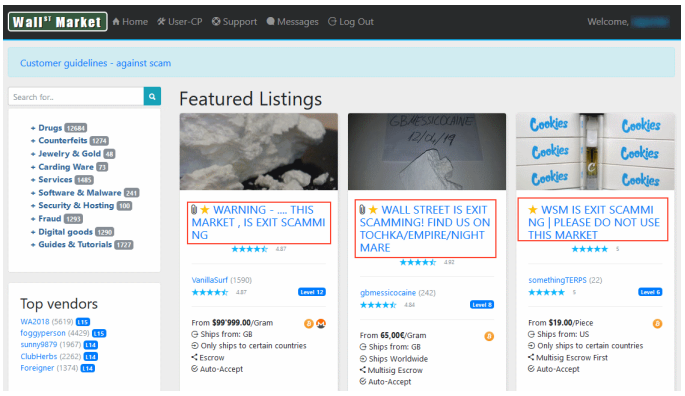

Figure 2.3: Image of Wall Street Market's front page. Note the renamed listings warning users of a suspected exit scam [13]

drew the attention of German and American law enforcement agencies, who took advantage of the chaotic situation to track down the main operators of the market[15].

2.4.4 Berlusconi Market: exit scam

Named after the former prime minister of Italy, Silvio Berlusconi, Berlusconi market was a fast-growing market platform and was one of the few remaining larger markets extant in the darknet ecosystem. The number of listings especially increased after the shutdown of Dream Market and Wall Street Market, with the number of drug listings almost doubling since the shutdown of Wall Street Market to 28,500 listings.

Until recently, Berlusconi was also one of the few markets to have weapons as part of its catalogue. While other markets might sell weapons such as tasers, or perhaps ammunition for 9-millimetre weapons, Berlusconi offered long guns such as AK47's or M16 style platforms[10].

In October 2019, users, and as was later revealed, market moderators, were unable to access the market platform because they were not able to successfully fill in the CAPTCHA required to enter the market. This situation continued for several days, with several users and the operators of the popular Darknet URL database dark.fail stating on their website that a possible exit scam was taking place[39]. As of the writing of this thesis, this situation is still developing, and people are still debating whether this is a true exit scam or whether the administrators have been arrested.

2.5 Other darknet market platforms

Several market platforms were reviewed in the process of this thesis. At the start of this thesis, the biggest extant market by far was Dream Market, followed by Wallstreet Market. So at the start, these two markets were the primarily market platforms used to research market platform practices. Over the course of the thesis, these market platforms were shut down by the authorities, however. This lead to a large increase in the number of listings on medium-sized markets such as Empire and Berlusconi market. A new market platform also appeared over the course of this thesis, namely Cryptonia market. The users of these last three markets were used as subjects of the survey, as the majority of listings present on the darknet could be found here and so could the majority of sales. These market platforms are described in more detail in the appendix.

2.6 Trust mechanisms enforced by market platforms

In order to for users to establish trust among each other, market platform administrators have developed a range of market platform functionalities to help achieve building that trust. These

features help to make their platforms more attractive both for buyers and vendors, and try to minimize the problems that are inherent to an underground market in illicit goods. Many of these features serve to protect both the buyer and the vendor from scams, as due to its anonymous and unregulated nature, the Darknet is rife with such attempts. Administrators hope that through these features, buyers and vendors can establish enough trust in order to create a vibrant market with a large number of transactions. As commissions on sales are the primary means a market platform has of making a profit, exit scams notwithstanding, administrators themselves also have a stake in ensuring that their platforms are seen to be as trustworthy as possible.

2.6.1 Feedback system

Because a Darknet market is an anonymous, low-trust environment, and scams are rife, legitimate vendors take great pains to build their brand and their reputation as a trustworthy vendor. One major way in how vendors establish their reputation is with the rating systems that all market platforms feature. With this system, buyers can give their purchases a score between 1.0 and 5.0, with 5.0 being the highest score. The aggregate score is then shown on the profile of the vendor, visible to all users of the platform.

This reputation for trustworthiness is seen as important by most vendors, and negative feedback is generally badly received. Usually, vendors will only consider a dispute or offer a refund or resend if the buyer in question has not already left an unfavourable rating or review.

Vendors also attempt to write about their previous activities on their profile pages, if possible. Vendors that migrated here from now-defunct markets like Hansa or AlphaBay might try to leverage the reputation they had on those markets to continue building their brand in this new marketplace.

2.6.2 Reviews

As the Darknet is a low-trust environment, buyers are at a severe disadvantage when placing orders, as the legal recourse to scams that exist in conventional markets do not exist on the Darknet. Another disadvantage is the major information asymmetry between buyers and vendors. Furthermore, the buyer does not know whether the vendor is a scam artist or not, as a scam cannot usually be detected from first glance. The buyer also does not know from first glance whether the product they're buying is of acceptable quality, or that the delivery method is sufficiently shielded from intervention by law enforcement.

To combat this, most Darknet markets implement a review system, where buyers can post text reviews and rate any purchase they have made. These reviews are prominently shown in both the page of a listing and on the profile page of the vendor. Using these, a buyer can decide whether the product is of sufficient quality, whether the package has sufficient countermeasures to evade detection by law enforcement (termed "stealth" by Darknet users), and how helpful the vendor was during the transaction.

All involved parties, the vendors, the buyers, and even the markets themselves, seem to place great importance on posting reviews and the quality of said reviews. Most markets recommend posting reviews in their purchase guidelines and when having problems with a transaction, discussing this problem with the vendor first before leaving a negative review. Vendors also seem to place some importance on the quality of reviews they receive. Most vendors offer at least a partial reimbursement in the case of an intercepted or lost shipment, but only when the buyer contacts them first to resolve this issue before posting negative ratings or reviews. The buyer forfeits the right for reimbursement from the vendor in case of a negative review. This shows that vendors go to some pains to prevent negative reviews from showing on their profile in order to maintain their reputation.

2.6.3 Escrow

Escrow is the process where two parties complete a transaction under low trust conditions by involving a third party which is trusted by both parties. The third party will hold the money for that transaction from the buyer, and when the transaction is completed, will transfer that money to the vendor. The trusted third party in Darknet transactions is usually the market itself. All markets offer such an escrow service, and highly recommend all buyers to participate in it in order to stop themselves from getting scammed. A visualization of this process can be seen in Figure 2.4.

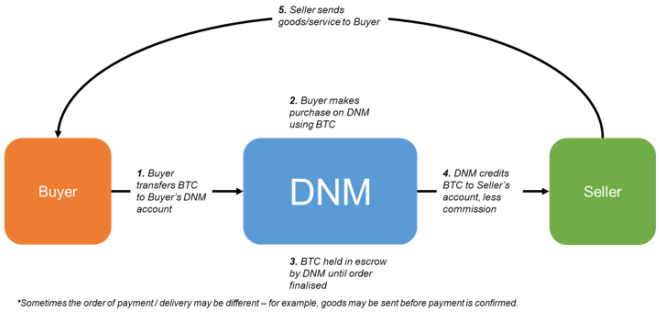

Figure 2.4: A visualization of the escrow process [31]

Most markets will hold the money in escrow for a set amount of time before the money is automatically sent to the vendor, usually around 14 days. In case of a dispute, the market usually makes the final decision and decides to either return the money to the vendor or finalize the transaction.

Escrow services are not flawless, however. There have been several occasions where the trusted third party, the market in each case, simply took all the Bitcoins they had in their possession and ran, more commonly known as an exit scam. One of the biggest scams, by the amount of money stolen, was the exit scam performed by the Evolution market. On March 2015, the operators of the Evolution marketplace froze its user's escrow accounts and stole around 12 million US dollars worth of Bitcoin[45]. In April of 2018, the operators of Wallstreet Market were also suspected of perpetrating an exit scam, stealing over 11 million dollars worth of Bitcoin from the market's escrow account[15].

2.6.4 Multisignature escrow

Multisignature (multisig) transactions are an evolution of the escrow system that was in use by the majority of Darknet markets at the time. Due to the large number of exit scams that took place on several large markets, an attempt was made to improve the escrow process in order to improve customer trust. The result was the 2/3 multisig system, made possible by using a cryptocurrency like bitcoin.

An overview of how a multisignature escrow transaction takes place is shown in figure 2.5. When a buyer wants to place a transaction, they send the money to a multisig address which requires at least 2 of the 3 signatures from the set {buyer, vendor, admin} in order to withdraw the money. If the purchase is completed successfully, and no party wishes to dispute the transaction then the buyer and vendor's signatures are sufficient in order for the vendor to redeem the money. If there is a dispute, however, then the admin can use their signature together with who they believe is the wronged party in order to return or give the money to them.

Using multisig, the chance for exit scams are reduced, as the third party now no longer has the ability to simply empty the escrow account themselves and claim the money as collusion with many vendors would now be needed to do so. This is useful in increasing trust between all parties

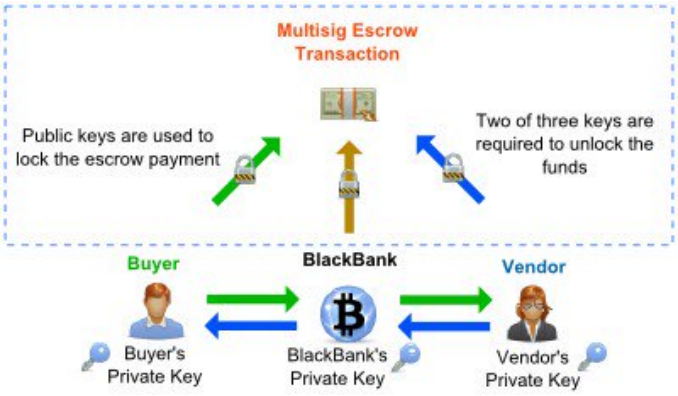

Figure 2.5: A visualization of the multisig escrow process of the BlackBank platform [18]

in a transaction, as the fewer opportunities exist to manipulate the transaction in some way, the more safe buyers will feel in making purchases.

2.6.5 Finalize early

Another service, or perhaps lack of service, that buyers can opt in to what is called finalize early. Through this method, the escrow system or multisig systems of a market is circumvented, leading to faster transactions, but giving the buyer no recourse should the vendor turn out to be a scam. Instead of waiting for confirmation through the usual escrow process, the market will simply deposit the money in the vendor's account after the order has been shipped. In the event of a lost or intercepted shipment, or the vendor turning out to be fraudulent, the buyer's money is lost and the market will not reimburse them. Most reviewed markets offer such an option but strongly recommend against it unless the vendor is highly trusted by the buyer. Most platforms heavily restrict the use of finalize early, only allowing verified accounts to do so, and not allowing finalize early on transactions already under escrow.

Opting for finalize early allows buyers the option to expedite their transaction, leading to potentially shorter delivery times. From the perspective of the vendor, it guarantees payment, as the funds have already been deposited in their account, so they get paid in any event. This does leave buyers open to a potential scam if they do choose to finalize early, as the vendor can simply receive the money and then not send the product. Therefore markets recommend buyers to only use finalize early when involving transactions with vendors they fully trust.

FE seems to be a matter of some contention in the darknet community. Several news websites recommend to not use finalize early, as its use leaves buyers more easily susceptible to scams[14][30]. Users themselves seem to experience issues with finalize early as well. A study covering the darknet behaviour of Swedish Darknet users asked respondents to rate a list of issues with Darknet markets they experienced and in that list issues related to finalize early were rated as the most common. [24]

2.6.6 Wallet-less escrow

A feature that is so far only present on Cryptonia market. A wallet-less escrow based market platform does not have a central escrow account used for every transaction, but instead creates a separate Bitcoin address for every single transaction.

According to the creators of Cryptonia, the process works as follows:

> "When you create an order we'll generate a unique Bitcoin address for your order. The private key for this address are[sic] not stored on our servers. Instead it will be generated when the order is finalized. This means we never really take posession[sic] of your funds."[4]

The creators claim that this removes the ability for Cryptonia to perpetrate an exit scam, but this is incorrect. The process as defined by the Cryptonia creators is not actually possible with the current systems in place, as it is impossible to derive the private key and it has to be generated at the same time as the address. If Cryptonia did possess such an ability, it means that they have found a way to derive the private keys of arbitrary Bitcoin addresses, thereby having compromised the entire Bitcoin infrastructure.

Ultimately, this system seems to be a marketing tactic more than anything else, although it does remove the risk associated with exit scams somewhat. As there is no central escrow account for users to store their Bitcoin in, there are no "dead" Bitcoins stored in such an account and users can only lose the Bitcoin they used in current transactions during an exit scam.

2.6.7 Organic trust-building mechanisms and technological trust-building mechanisms

After researching these trust-building mechanisms, a divide between two main groups can be made. In this thesis, these two groups will from now on be called organic trust-building mechanisms, and technological trust-building mechanisms.

Technological trust mechanisms include mechanisms such as PGP encryption on private messages, different types of payment methods such as finalize early or multisignature escrow, or anti-phishing measures. These mechanisms tend to be based on technology-based solutions to privacy issues, as they attempt to use encryption, or CAPTCHAs or other forms of digital solutions to ensure both authenticity and privacy.

Organic trust mechanisms include mechanisms such as review scores, comment systems and any other mechanic that allows buyers to directly or indirectly communicate both with vendors and with other buyers. These mechanisms are more community-based than technology-based, although of course these mechanisms are all implemented digitally as well. These mechanisms allow users to create a community between vendors and their prospective buyers, which allows vendors to increase their sales and buyers to have their prospective purchases be validated by other buyers.

All market platforms incorporate the same organic trust mechanisms in their design. All reviewed market included a comment section and the ability to give feedback to a vendor in the form of a star review.

Not all technological trust mechanisms are present in all markets. Multisignature escrow was not available on Berlusconi market, for example, and only Cryptonia has a wallet-less based escrow system which it uses to create trust in its infrastructure. Because each market has its own implementation of technological trust mechanisms, it also requires the users to place trust in the market themselves that these features work as advertised. Placing trust in a market's escrow system, for instance, requires users to both trust the market administrators to be capable enough to properly set up such a system without any intentional security flaws. Users also have to trust the market administrators not to perpetrate an exit scam, as an escrow system puts a lot of power over the transaction into the hands of the market.

2.6.8 Factors relevant in market selection by users

This section will contain several factors which users might find important when visiting a market. Factors relevant to both buyers and vendors will be discussed.

Buyers and vendors choose to use these markets, and engage in criminal activities, for several reasons. [16] states that criminals engage in rational choice theory, calculating the costs and benefits of their activities and making decisions based on those calculations.

One major difference between traditional drug trading and Darknet markets is the separation between vendor and buyer. As was already discussed earlier that it could potentially lower the violence inherent in the drug trade, there are also some other factors that could change the cost/benefit balance for potential buyers and vendors. The first one is that the distance between buyer and vendor and the anonymity could help alleviate any feelings of guilt the vendor might

have [25]. Furthermore, due to its online nature, the probability for seizure by authorities is considered to be lower than in-person sales, and generally, people consider the probability of the punishment happening to have greater weight than the harshness of said punishment[25][32].

The main benefits gained from these activities are the financial incentive on the part of vendors, and the desire for recreational drugs on the part of the buyers. As the (perceived) probability of detection by law enforcement is considered low, the costs associated with their activities are mainly social in nature, such as spending time online they could have spent with legitimate employment or personal relationships.[26].

2.7 Implementation of trust-building mechanisms on various markets

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

Figure 2.6: An overview of the payment methods available on various Darknet market platforms [19]

Figure 2.6 shows the various means of payment available to the listed market platforms. As can be seen from the Figure, The differences in payment methods are minor. All reviewed markets are classic escrow markets with the only difference being the type of cryptocurrency they accept or the implementation of multisig. Tochka is anomalous in that it does not directly accept the most common cryptocurrency, namely Bitcoin.

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	?

Figure 2.7: An overview of the security measures available on various Darknet market platforms [19]

Figure 2.7 shows the various security measure available on the listed market platforms. As can be seen from the Figure, Dream market offers the most varied number of security options, while other markets lag behind. Tochka especially does not offer a great number of varied security features, nor does it supply a list of verified alternative mirrors in case of the main site shutting down.

Figure 2.2 shows various security and payments aspects of the listed markets. As can be seen from the Figure, a feedback system and PGP keys to identify vendors are implemented across the board. It also shows that multisig is implemented in the majority of cryptomarkets. Most of the largest markets, those being Dream Market, Berlusconi, and Empire market, seem not to have implemented multisig, apparently believing that standard escrow is good enough for their purposes. Acceptance of the standard Bitcoin protocol is also very high, with implementation of Monero (XMR) being a close second.

	anti-phishing	PGP	level	awards	buyer info	feedback	cross verifiable	partnership	BTC	BCH	LTC	XMR	ETH	FE	Multisig	vendor bond
Wall Street	x	x	x	x	x	x		x	x			x			x	$150
Dream	x	x				x	x		x	x		x		x		$700
Empire	x	x	x		x	x			x		x	x		x		$100
Cryptonia	x	x	x			x	x	x	x			x		x	x	$45
Berlusconi	x	x				x	x		x		x	x		x		$400
Tochka		x				x		x	x	x			x	x	x	$100
Olympus	x	x	x			x	x		x			x		x	x	$300
Libertas		x				x						x			x	
CGMC		x			x	x									x	
Zion		x				x			x			x		x	x	$300
Apollon	x	x	x			x			x							$200
Rapture	x	x				x			x			x		x	x	$250
Serpent		x	x			x			x			x		x	x	$225

Table 2.2: Summary overview of various Darknet market platforms [19]

In this table, "cross verifiable" stands for the functionality for a vendor to verify themselves as a vendor of other markets. A vendor on Cryptonia, for instance, can verify themselves as also being active on other markets, and can even show their average rating score on their profile page. Such a functionality allows markets and vendors to "piggyback" on the perceived trustworthiness of other market platforms, as vendors can now leverage their perhaps larger presence on other markets to build their customer base in new market platforms.

Chapter 3

Methodology & Implementation

Recall that the overall research question of this thesis is as follows:

> **RQ:** What mechanisms underlie the trust-building dynamics in underground market platforms?

In order to properly answer this question, several different kinds of data will have to be gathered. To gather the data necessary for a quantitative overview on what the Darknet community thinks of the various trust-building mechanisms, simply gathering statistical data from the market platforms themselves is not enough. The community itself will have to be contacted. A survey was seen as the best means of gathering that kind of quantitative data directly from the community, and the process through which that survey was created and distributed will be discussed in section 3.3.

As the survey could not be distributed to the entire Darknet community via automated means, as will be discussed further in the survey distribution section, a method of creating a representative sample of the various market platform communities also had to be devised.

Firstly, a means to gather the raw HTML data from each market platform had to be devised. Secondly, the raw data had to be processed such that any useful information could be extracted from it. This was done firstly through parsing the raw HTML data that was gathered, and subsequently training an LDA model on that parsed data in order to categorize the vendors of each market platform. Furthermore, some additional statistical information such as the total amount of listings and vendors was also extracted. This entire process will be further described in section 3.2

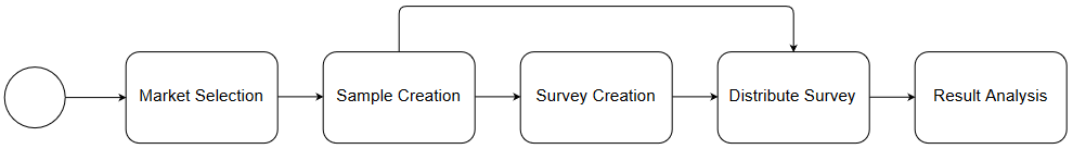

Figure 3.1: The process of data collection and analysis

Figure 3.1 shows a general overview of this process, and each part will be further described in the following sections.

3.1 Market platform selection

As of the writing of this thesis, Empire Market and Cryptonia are the two largest Darknet markets that are currently operational after the shutdown of Wall Street Market and Dream Market. Because of this, these three markets were chosen as the basis for this study. At the start of this

thesis, Wall Street Market and Dream Market were both operational, but over the duration of the thesis project, both markets were taken offline. Dream market was taken down by law enforcement, and Wall Street market committed an exit scam before having its owners be arrested.

In order to replace these 3 markets that were shut down, Cryptonia and Empire were chosen as they are the largest remaining markets, and saw a large increase in vendors and listings ever since Berlusconi, Wall Street and Dream markets were shut down. While Berlusconi market and Wall Street Market were shut down, it was still possible to scrape the market platforms, as that process was completed before the market platforms were shut down.

3.2 Sampling participants of underground market platforms

In order to create a representative sample of the vendors of the underground markets, a dataset containing the profiles of all vendors and listings of the reviewed markets was compiled. To accomplish this, a script was written in Python that would first index the marketplace and retrieve the URLs of all drug offers and their respective vendors, and continue with downloading the offers and vendors that were found. An overview of the process can be seen in Figure 3.2. Further information about these markets can be found in the appendix.

3.2.1 Scraping process

To extract the raw HTML data from each market, the chosen market platforms would have to be scraped. Data scraping is the act of harvesting data from a web server. As every market required a session cookie in order to enter it, an account was created for each market. As a login also included a CAPTCHA, this login was performed manually in order to create a session cookie. This session cookie was then transferred to the Python script for it to act as a normal user of the market.

While Wall Street Market and Berlusconi market have been taken offline, the scraping process was still successfully completed, and therefore its data was also included in the data analysis process.

The scraping process was performed in two stages. In the first stage, every page of the drugs section of a darknet market was scraped for every profile and listing URL that could be found. In the second step, these URLs would be scraped in order to extract the actual data. The form of the data was a copy of the raw HTML code of each listing and profile page. This was done in order to ensure that the data would remain available in the event of a Darknet market experiencing slowdowns or were offline for any reason.

3.2.2 Data extraction process

In order to process the raw HTML data gained from the scrape, the data was first parsed in order to generate a dataset that the LDA model could work with. Firstly the HTML data was parsed by a second python script which retrieved all useful information from each vendor page, such as vendor name, vendor PGP key etc. After this parsing process was completed, an LDA model was employed in order to categorize the vendor profiles and listings into various drug categories. LDA (Latent Dirichlet Allocation) is a form of topic modelling which attempts to extract from each document, here defined the title of an individual drug listing, several topics and creates these topics from the words present in said document.[8]

This model was then used to categorize the vendors by the drugs that they sold. Every drug listing was given a category, and the vendor associated with that listing was placed in that category. As some vendors sold multiple types of drugs, some vendors had multiple categories associated with them.

In order to prepare the data for the LDA model, the HTML data was first parsed to extract all useful information from it. In the case of profiles, there were several factors that were of interest, namely: profile name, PGP key, finalize early allowance, trusted vendor status, Shipping data,

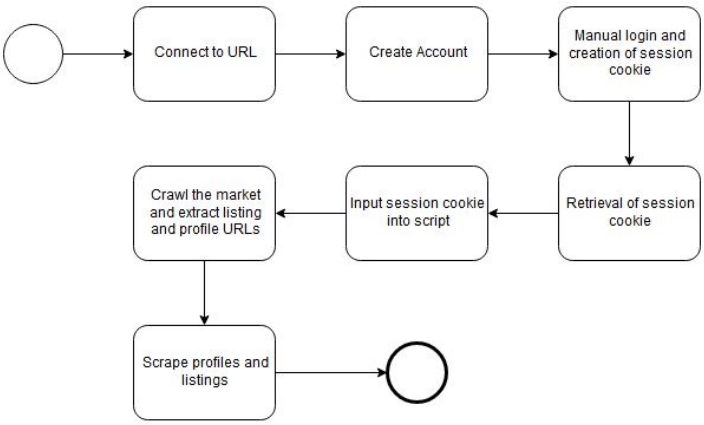

Figure 3.2: Data collection process

reviews, number of completed trades, average review score, age of account, amount of disputes won/lost, amount of feedback, profile description. Not all markets show exactly the same statistics on all vendors, therefore, dimensions which are present in all markets were prioritised.

For the data that was input into the model, firstly all the data was stemmed and lemmatized. This process removes all stop words and reduces each word to their root form. Words shorter than 4 characters were also ignored, with the exception of certain abbreviations associated with various drug types, such as XTC, LSD, THC or similar terms.

As an example, the listing "x South Park LSD Blotter ug" would be reduced to ['south', 'park', 'lsd', 'blotter'] which could then be input into the model.

3.3 Survey

To obtain the quantitative data required in order to be able to theorize about trust-building mechanisms, speaking to market platform users themselves is required as the markets do not track such information themselves. Or if they do, they do not publish it. Therefore, to gain this data, a cross-sectional survey was created and sent to market platform users.

3.3.1 Survey creation

One of the main requirements of the survey was ensuring that the respondent rate was as high as could be achieved. To achieve this, one of the aspects that was considered to be most important was safeguarding the anonymity of the respondents and ensuring their responses were kept secure and out of the hands of third parties.

Therefore, the survey was created using LimeSurvey, a free and open source on-line statistical survey web application. The survey was hosted as a tor hidden service on one of the servers of the Eindhoven University of Technology. Furthermore, the decision to put the survey on a Tor hidden service was made in order to convince the target sample that the survey would be as anonymous as possible, and to establish that we had a minimum level of competence in relation to Tor in order to instill more confidence.

Beyond its rich feature set and free nature, LimeSurvey was also used because we could host the database of all the completed surveys ourselves and therefore maintain total control of the data. Something that is not possible when using other surveying tools such as Google Forms.

3.3.2 Survey structure

The survey consists of several sections. The main page, as seen in figure 3.3, contains a small bit of text stating the intent of the survey, and some general information such as the amount of questions in the survey and an estimation on how much time the survey takes to complete.

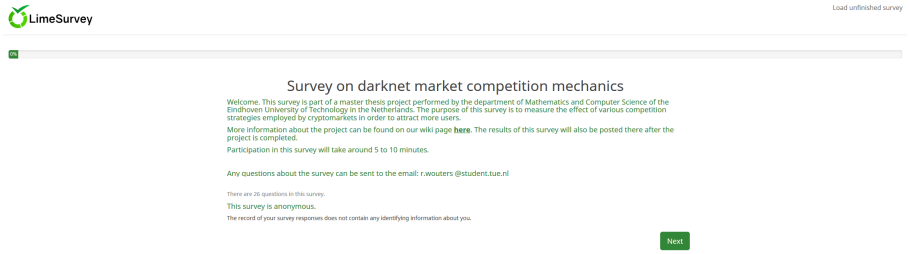

Figure 3.3: A screenshot of the front page of the survey

Section 1 contains questions about the general darknet usage of participants. Section 2 contains more specific questions about how the participants interact with darknet markets and the various features of those markets. These two sections feature a mix of closed multiple-choice questions allowing participants to rate the perceived usefulness of various darknet market functions and open questions which allow participants to describe what they consider to be the most important aspects of a darknet market with respect to their business. An example of these questions can be seen in Figure 3.4. Section 3 contains general demographics questions mostly consisting of closed questions. Section 4, the last section, contains a question regarding participant's willingness to participate in a further in-depth interview.

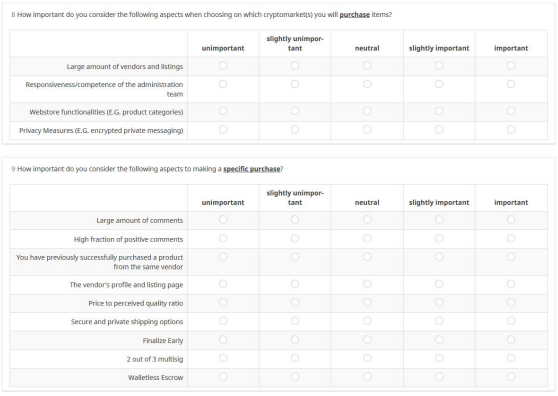

Figure 3.4: A screenshot of some questions from the survey

Sections 1 and 2 are meant to gauge which trust-building mechanisms users value the most, which market platforms they use, and what lead to them choosing those specific market platforms. Furthermore, it also contains questions on how various market platform shutdowns have impacted their Darknet usage, if at all. The purpose of section 3 is to gather information about the general demographics of darknet users.

3.3.3 Survey distribution

One further aspect important to the success of the survey was ensuring that the survey was properly distributed to the Darknet community. Several avenues were used in order to distribute the survey to darknet users. Posts were created on Darknet market-focused communities both on the darknet and the clearnet. Envoy forum, The Hub, Dread and Reddit were all used to approach Darknet market users and make them aware of the survey. An example of the message posted on

these forums is shown in Figure 3.5. As the users of these communities were primarily buyers, a more direct method was employed to approach vendors on the various Darknet markets. Using direct messages, vendors on Berlusconi market, Empire market, Tochka market and Cryptonia market were approached in order to reach as many vendors as possible. As the process of sending direct messages could not be automated, because one has to fill in a CAPTCHA for each private message, it had to be done manually. This, coupled with the slow loading times of some Darknet markets, means that only a sample of the entire vendor-base could be approached.

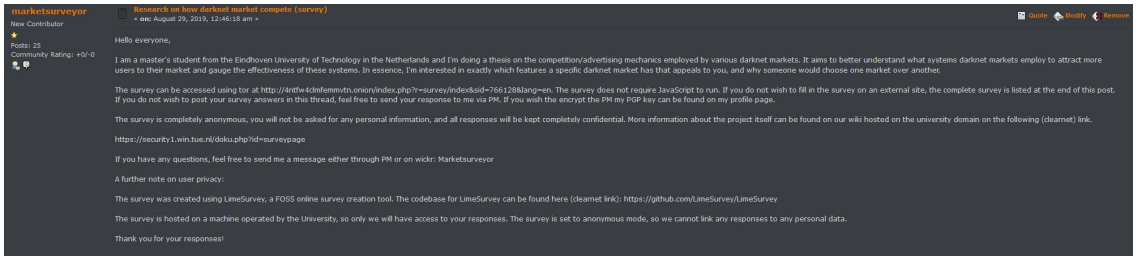

Figure 3.5: A screenshot of the message posted on the Hub

The vendors on the darknet markets were sampled according to the result of the market measurements that were gathered beforehand. In order to attempt to get a representative sample of the entire vendor population of a Darknet market, the vendors were selected to proportionally represent their type of drug they sell. For instance, if the vendor population of market A contained 60% heroin vendors and 40% ketamine vendors, the sample would also consist of users identified as such vendors in the same proportion. Out of all vendors, a sample was then created and that sample was then contacted by the private message functionality of each Darknet market.

The different samples that were taken from the various Darknet markets were derived from the measurements and statistics taken by the LDA model, the results of which can be found in Chapter 4. The drug categories it generated were used to categorize the drug vendors found on each market, and from those drug vendors a representative sample of the entire market was created, and that sample was then sent private messages through the market themselves. This approach was chosen in order to maintain some form of representative sample, as, due to the CAPTCHA required in contacting the vendors, simply generating a large amount of private messages was not possible.

Chapter 4

Results

4.1 Descriptive statistics of selected market platforms

After the data collection phase, the data were analyzed in order to create several subgroups of listings and users which would then be used to create samples of the population which would then be targeted by the survey. This allows us to send the survey to a representative sample of the entire drug vendor community on the major Darknet markets.

Market	**# offers**	**# profiles**
Tochka	2514	346
Wall Street Market	11864	2014
Berlusconi Market	13211	526
Empire Market	7722	447
All markets	35311	3333

Table 4.1: Results of the scrape

Initial data about the scrape results can be seen in table 4.1. As can be seen from the table, Tochka is a much smaller market compared to Wall Street Market or Berlusconi market, with only having around 2000 drug offers in total. As can also be seen from the table, Berlusconi Market seems to have a very high listing/vendor ratio. This could be explained because the Berlusconi market creates separate entries for the same listing sold in different quantities. "Xanax bar 20 mg" will be a separate listing from "Xanax bar 40 mg", for example.

name	vendor	shipsfrom
G CANADIAN BROWN SUGAR MDA FE	Empyrean	United States
Adderall mg XR	Greatdeals	Worldwide
potassium cyanide powder g	sabastien	United States
LYRICA pills Pregabalin mg	DoktorSommer	Germany
LYRICA pills Pregabalin mg	DoktorSommer	Germany
LYRICA pills Pregabalin mg	DoktorSommer	Germany
LYRICA pills Pregabalin mg	DoktorSommer	Germany
LYRICA pills Pregabalin mg	DoktorSommer	Germany
LYRICA pills Pregabalin mg	DoktorSommer	Germany
Trenbolone Acetate mgml ml Bioniche	SteroidWarehouse	Netherlands
Purple Aliens mg	boomers	United Kingdom
G CANADIAN BROWN SUGAR MDA ESCROW	Empyrean	United States

Figure 4.1: An example of listings parsed from Berlusconi market

Figures 4.1 shows an example of the parsed data gained from listing pages. As can be seen

Category	Keywords identified by the LDA topic model
Cannabis	'0.111*"haze" + 0.070*"weed" + 0.052*"amnesia" + 0.051*"super" + 0.033*"lemon"'
Cannabis	'0.096*"hash" + 0.063*"gram" + 0.053*"thc" + 0.052*"vape" + 0.048*"cartridg"'
Heroin	'0.104*"heroin" + 0.045*"cooki" + 0.036*"afghan" + 0.032*"qualiti" + 0.032*"black"'
Pharmaceuticals	'0.106*"powder" + 0.061*"capsul" + 0.058*"best" + 0.050*"purpl" + 0.044*"cart"'
Xanax/Pharmaceuticals	'0.108*"xanax" + 0.061*"tablet" + 0.046*"offer" + 0.042*"viagra" + 0.040*"alprazolam"'
Amphetamines	'0.147*"speed" + 0.087*"past" + 0.079*"amphetamin" + 0.051*"valium" + 0.041*"seed"'
Meth/Ketamin	'0.085*"ketamin" + 0.076*"crystal" + 0.072*"tab" + 0.061*"meth" + 0.054*"indoor"'
XTC/LSD	'0.129*"xtc" + 0.083*"lsd" + 0.074*"thc" + 0.069*"mdma" + 0.049*"blotter"'
Cocaine	'0.164*"cocain" + 0.121*"qualiti" + 0.103*"high" + 0.093*"pure" + 0.058*"gram"'
Pharmaceuticals/MDMA	'0.217*"mdma" + 0.082*"dutch" + 0.060*"pharma" + 0.052*"oxycodon" + 0.049*"pure"'

Table 4.2: The topics the LDA model discovered in the dataset and their manual categorization

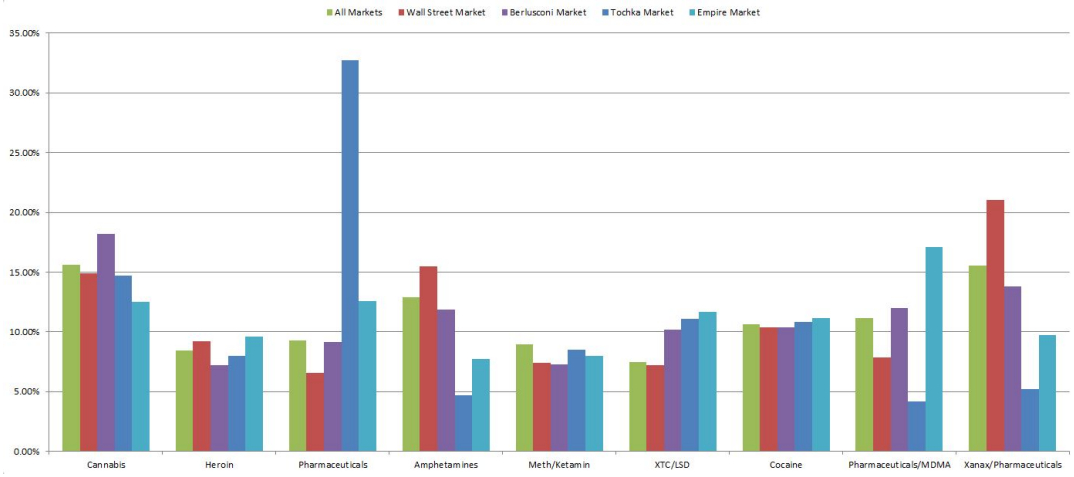

Figure 4.2: All drug listings categorized by topic according to the LDA model

from the figure, some fields are either left blank by the vendor, or are in a language other than English. For the purpose of this thesis, non-English profiles were ignored.

Table 4.2 shows an example of a set of topics that the LDA model generates when trained on a dataset. As can be seen from the table, cannabis or terms related to cannabis make up a large proportion of the dataset, meaning that some drug types that were not represented as often in the dataset, such as heroin or LSD, were also included in some topics. Another explanation for this could be that there are a large number of cannabis strains each with their own specific names that the model had difficulties with classifying. The word "blue" in the first topic of the table, for instance, refers to the "Blue Dream" strain of cannabis and is therefore included in that topic. This concurs with the results shown in Figure 2.1, where cannabis was the largest proportion of darknet sales.

Figure 4.2 shows an overview of all drug listings categorized by the different vendor categories created by the LDA topic model. An overview of these categories can be seen in Table 4.2. As can be seen from the Figure, the pharmaceutical drugs and cannabis topics are the largest topics, with the other topics save amphetamines having a roughly equal share. It is interesting to note that Tochka market seems to have a far higher number of Pharmaceutical drug listings, while having a much lower number of amphetamine offers.

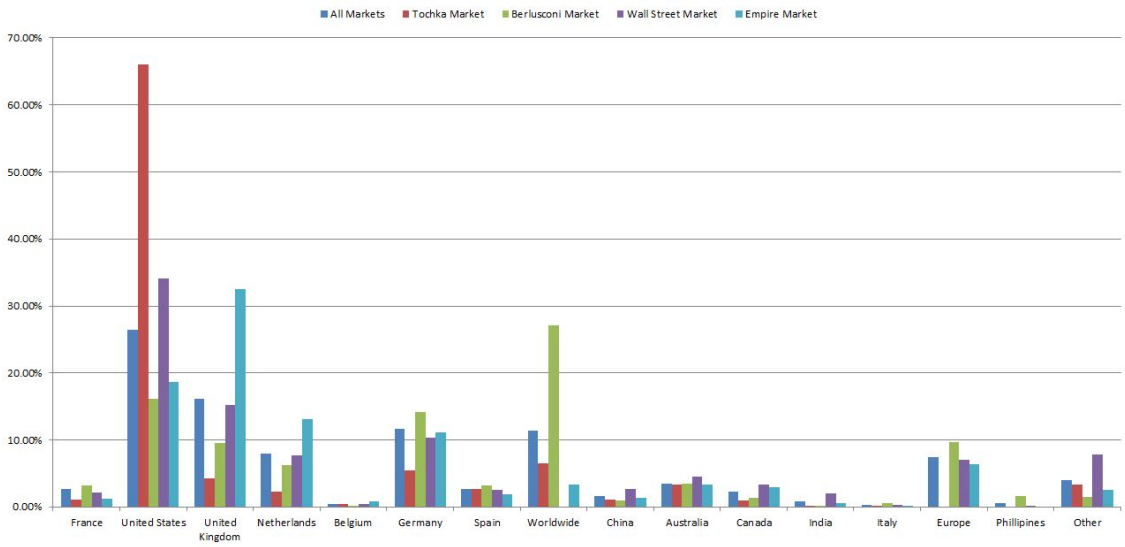

Figure 4.3: All drug listings categorized by origin country

Figure 4.3 shows an overview of all drug listings categorized by the nations these listing are shipped from. In this Figure, 'other' was defined as any country that had less than 100 total listings over the entire dataset. As can be seen from the Figure, the majority of listings either originate from the United States or the United Kingdom. Germany and the Netherlands are also the originating countries of a substantial number of listings, with those two countries having more listings than the rest of Europe combined. The Netherlands especially has a large number of listings when takings its comparatively small size and population compared to other countries such as the US, the UK or Germany into account.

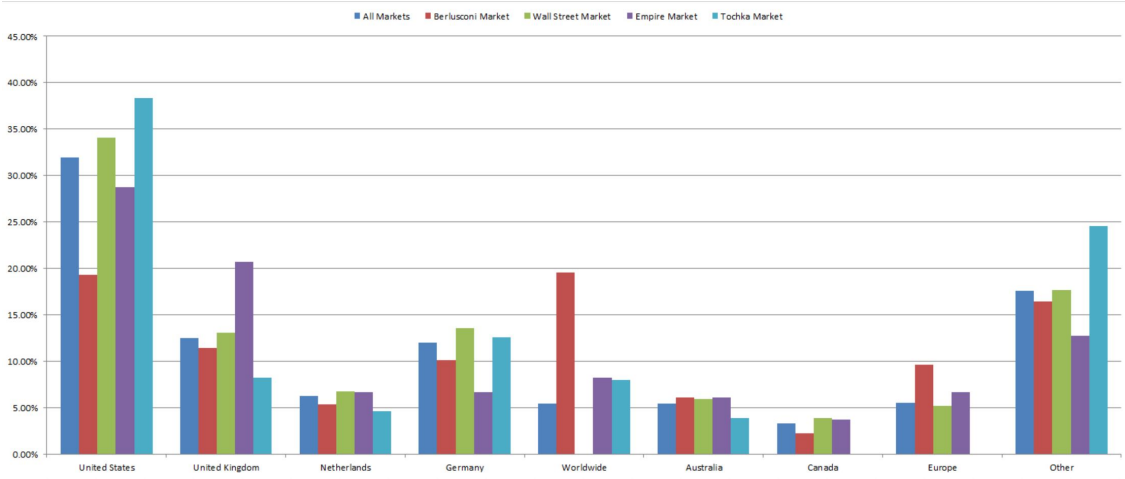

Figure 4.4: All profiles categorized by origin country

Figure 4.4 shows an overview of all profiles categorized by the nations their listings are shipped from. In this Figure, 'other' was defined as any country that had less than 100 total profiles over the entire dataset. Note that some profiles have multiple origin nations dependent on their specific listings. Especially noticeable in this Figure is that the number of profiles from Tochka market originating from the United States is far lower than its listings, and the worldwide profiles much higher. This could mean that the vendors in the United States have more listings per profile on average than vendors from other nations.

4.1.1 Market platform user migration

Over the course of this thesis, several market platforms have become defunct. Dream Market was shut down by the authorities, and Wall Street Market and Berlusconi Market performed an exit scam. With the loss of these markets, at the time among the largest market currently extant, a great increase in listings and new users could be seen in the remaining markets. From this, it can be inferred that unlike the Hansa and AlphaBay takedowns, these market platform takedowns were seen as business as usual by the community and did not lead to people lowering their Darknet market usage.

Berlusconi saw its number of listings increase by over 200%, from 14,000 to over 28,000, before it too exit scammed a few months after Wall Street Market and Dream Market were taken down. Empire Market and Cryptonia market, in particular, saw a great increase in its number of listings, with Empire market seeing an increase of more than 500% from 7,700 listings to more than 37,000 listings.

4.2 Survey results discussion and analysis

In order to gather responses for the survey, the survey was posted to several forums and sent via personal message to a selection of vendors on Empire market, Berlusconi market, and Cryptonia. Forum messages were posted on /r/darknet, The Hub, and Envoy forum. The administrators on Dread were also contacted but they did not respond. 204 Vendors were approached on Berlusconi, 142 vendors on Empire, and 217 vendors on Cryptonia. Response rates were, as expected, very low. Only 5 vendors responded and 8 buyers responded. The forum thread on the Hub was read 647 times as of the 27th of October, and the Envoy forum thread 269 times. Reddit does not track such statistics.

Several survey questions will be referenced in the following sections. The full list of questions can be found in the appendix.

4.2.1 Respondent characteristics

Gender

Of all the respondents, the overwhelming part identified as male, with only a single person responding as female. The single female respondent's responses did not significantly differ from the general trend.

Respondent age

The respondents were primarily composed of young adults, as 8/13 were in the 19-30 age range, with 4 being older and one person (the single female respondent being younger).

Respondent age	Count
< 18	1
19-30	8
31-40	2
41-50	2
51-60	0
> 60	0

Table 4.3: Respondent's age

From looking at American drug use statistics, the primary age group of drug users in their statistics are the ages between 16 and 30, with the percentage of drug users falling off as people age [34], and our sample roughly corresponds with that. The few vendors that responded also tended

to be older than the buyers, especially the vendors who cited their Darknet market activities as their primary means of income, of whom 2 out of 3 were older than 30.

Respondent experience in digital security

When respondents were asked to assess their experience relating to digital security compared to the general population, they uniformly considered themselves more capable in digital security matters than the general population. Table 4.4 shows the results of the question. As can be seen from the table, not a single response was at "equal" or lower. While some of this can be attributed to people overestimating their ability, it does have some basis. To even be able to view a Darknet market, one has to both be able to access Tor through the browser, and be able to find an onion link to the market. Furthermore, they need to be able to complete bitcoin transactions, which is a non-trivial task for an uninitiated user.

Experience level	**Count**
Not experienced at all	0
Less experienced	0
Equal	0
Somewhat experienced	7
Very experienced	7

Table 4.4: Respondent's own assessment of their competence regarding digital security compared to the general population

Respondent role

Of the 13 respondents, all but 1 answered either "buyer" or "both" (buyer and vendor) at the role question, with those options standing at 8 and 4 answers respectively, meaning that the majority of vendors surveyed were also active as buyers.

There were only 6 respondents recorded who responded they participated in Darknet markets as a vendor. As the majority of the darknet user base are buyers and vendors are by necessity less likely to answer a survey as they are at higher risk of incarceration.

4.2.2 Overview of respondent's general darknet usage

The majority of respondents (10/13) were participating in Empire market, with Cryptonia market being the second largest. Berlusconi, while being ostensibly the second largest market by number of listings, only had 2 people participating in it. It should be noted that these responses were collected before the Berlusconi administrator allegedly exit-scammed and the market became unreachable.

Existing Market	**Count**	**Defunct Market**	**Count**
Empire Market	10	Dream Market	10
Berlusconi Market	2	Silk Road	4
Tochka	2	Wallstreet Market	8
Cryptonia	6	AlphaBay	2
Genesis	2	Hansa	6
The Majestic Garden	4	None	2
Other	3	Other	4

Table 4.5: Respondent's answers to the market participation questions

Of the respondents, as can be seen from table 4.5, the majority have either been part of Dream Market or Wallstreet market. Of all the respondents not answering with "none", every respondent

was a user of either Wallstreet Market or Dream Market at one point, showing that these markets were the dominant ones of their time. It also seems that the majority of the users from these markets migrated towards Empire and Cryptonia when the former two markets were shut down.

When answering whether the recent shutdowns of Wallstreet Market and Dream Market had impacted the respondent's Darknet market usage, most responded that it had not. One user responded with "markets are never safe". Another responded:

> *"All markets get shut down eventually, so moving to another one has been old hat by now."*

This respondent was also active in the old Silk Road marketplace according to their previous answers, showing that users frequently change markets and indeed expect their presence on the market and even the market itself to be of a very temporary nature.

4.2.3 Buyer specific preferences

Most valued trust-building mechanisms by buyers

When looking at the responses for "How important do you consider the following aspects to making a specific purchase?", the aspects that were rated the most highly were "Large amount of comments", "High fraction of positive comments", and "Had a previous successful transaction from this vendor". With 10/12, 9/12 and 10/12 of respondents rating these aspects as at least "slightly important" or higher respectively. This shows that creating trust between individual buyers and sellers is considered to be far more important than the technological aspects that darknet markets can create themselves.

When asked what respondents found to be the most important aspect to making a purchase, they also responded that the personal and collective creation of trust between vendor and buyer was more important than trust in the market itself. One user's comment was:

> *"If I know that a lot of transactions have already been rated highly it is less probably that I get scammed."*

adding weight to the theory that a feedback and comment system is crucial to establishing trust from both ends of the transaction. The buyers can see that the listing is most likely legitimate if a large number of previous buyers have already successfully completed a purchase. This also helps the vendors, as they receive useful feedback which can help them build their personal brand and it shows them that their stealth is appropriate.

Least valued trust-building mechanisms by buyers

The lowest rated aspects, on the other hand, were "Finalize Early" and "2/3 multisig", with 10/12 and 9/12 rating these aspects as "Neutral" or lower. Opinions on the importance of the vendor profile page were also mixed, with an almost equal distribution between all options. The ability to send encrypted private messages and other privacy measures created by a market were very highly desired, however. With 10/12 respondents deeming this to be "Slightly important" or higher.

Curiously, "wallet-less escrow" was rated as "slightly important" or higher by 8/12 respondents, even though only one currently active market supports such a feature. Although as previously discussed, wallet-less escrow is not necessarily less susceptible to an exit scam, people still seem to believe that it is, which could lead to this aspect being rated as more important than the other payment methods listed.

This could mean that users primarily care about any measures that stop their personal information from falling into the hands of third parties, and value specific market functionalities such as finalize early less as a lack of these has a far smaller worst-case impact than a loss of privacy would have (i.e. a log of their activities falling into the hands of the authorities).

Effects of market platform shutdowns on buyer behaviour

This can also be seen from the answers to the open question regarding what the respondents' biggest concern would be if a Darknet market was shut down by the authorities. Most buyers stated that they were unconcerned about their privacy being lost. Not because of specific darknet features, however, but due to their own op-sec practices.

Most respondents seem to be primarily concerned with losing the money they had already placed in the market's escrow accounts. As both currency placed there for future purchases and current purchases is now under the direct control of the market, and when that market gets shut down for any reason, that currency is lost.

Users were also concerned with the possible shocks the shutdown of 2 major Darknet markets could have to the entire Darknet market ecosystem. One user that was previously active on Dream Market decried the fact after the loss of Dream Market the lack of competition, or at least the smaller scale of competition, lead to an increase in prices. Whether this was correct has not been researched.

> *"price increases, decrease of reliable vendors, and sussing out new markets is a pain. I also worry that address'[sic] would be leaked but that is unlikely with good opsec..."*

They also consider the risk of exit scams to be a greater threat than actual law enforcement intervention. At least they believe that it is more likely for the administrators of a market to commit an exit scam than getting arrested.

> *"...Imo [in my opinion] markets are more likely to shut down due to other factors (exit scam, DDOS pressure, etc)."*

Indeed, from reviewing several communities on Tor discussing darknet markets, all markets seem universally distrusted with some users even believing that all markets are prospective exit scams.

Most respondents also consider themselves beneath the notice of the authorities if a shut down does happen. They believe that law enforcement will be primarily interested in arresting the market administrators and major vendors, and will not concern themselves with buyers who only purchase small quantities of drugs meant for personal use. A lack of concern that seems legitimate, as buyers purchasing small amounts of drugs very rarely get prosecuted even if their personal information was known.[43]

> *"I wouldn't feel any anxiety as my address will always be pgp encrypted and UK police aren't exactly gonna [sic] send a SWAT team out for some nobody buying personal amouns[sic]"*

Overall impressions on buyer behaviour

Ultimately, Darknet market buyers seem to attach the most value to aspects of a Darknet market that lets them create trust between them and specific Darknet market vendors, instead of creating trust in the entire Darknet market as a whole. Functionalities which can publicly show that, collectively, the user base considers a certain listing or a certain vendor to be legitimate appear to be highly valued, while aspects that try to inorganically create trust appear to be considered less important. They also don't seem to trust these markets with safeguarding their personal information and take their own measures to for instance encrypt their addresses with PGP in order to conceal their identity. They seem to consider their presence on one single market transitory, both due to frequent exit scams and the ever-present threat of law enforcement shutdowns. The recent spate of DDoS attacks against the largest Darknet markets might have also lead to some amount of frustration as users can't quickly discern between their funds being unavailable due to a DDoS attack or an exit scam, leading to much frustration and distrust between a Darknet market and its user base.

4.2.4 Vendor specific preferences

Income statistics

Of the 6 buyers, half stated that their Darknet market activities were their major source of income, with the other half responding otherwise. The ones responding in the affirmative also reported their income as higher than those for whom their Darknet market activities were not their major source of income. Of the 3 respondents, 2 reported their income as higher than 10,000 USD per month, while 1 reported their income as between 1,000 and 5,000 USD per month. Of the other half, their reported income was lower, with 2 selecting less than 1,000 USD per month and the last respondent giving no answer.

Most valued trust-building mechanisms by vendors

The most important aspect according to the vendors was the "ability to post comments", which was rated as "slightly important" or higher by all respondents, followed closely by "The responsiveness and competence of the administration team", which was rated as "slightly important" or higher by 5/6 respondents. The latter can be explained because vendors are more likely to more frequently engage with market administrators than buyers are, for whom the aspect was rated as "slightly important" or higher by only half of the respondents. Firstly to register as a vendor, and market administrators are needed to resolve any dispute between a vendor and buyer.

As stated previously in the thesis, vendors place great interest in ensuring that the comments on their products are as favourable as possible, with some vendors even withholding services like discounted reshipping if the buyer posts a negative comment without first discussing it with the vendor. This, together with the high scores for the feedback system, shows that like the buyers, vendors seem to highly value any aspect that enables them to create trust, as they believe this will lead to more successful sales. As one vendor said, "Reviews show everyone that the drugs are legit. And a lot of people don't buy drugs that have low scores".

Least valued trust-building mechanisms by vendors

Similar to the buyer's opinions, by far the least important aspect is finalize early, with all but one respondent deeming it "unimportant", with the last respondent deeming it "slightly unimportant". That vendors don't consider this aspect to be important is curious, as finalize early ensures that the vendor receives their money a lot quicker than if they employed a normal escrow transaction. It could be that finalize early is simply rarely used, so it is not considered a factor by either party. This is only conjecture, however, and no specific further questions about finalize early were part of the survey.

"Acceptance of coins other than bitcoin" was also lowly rated, with 4/6 respondents rating it as "neutral" or lower. "The number of potential buyers" was also rated as "neutral" by 4/6 of respondents. The reason for this could be that vendors have no means of actually checking how many buyers are active on a market. One of the respondents also stated that there is *"no way to know this"*.

Effects of market platform shutdowns on vendor behaviour

Unlike the buyers, who were mostly concerned about avoiding loss of currency through an exit scam, vendors are concerned with the loss of privacy, or arrest by the authorities. One of the buyer's main concern was "The cops accessing all the market's servers and tracking my location". Another vendor main concern was *"being caught ;)"* while another only answered "privacy". This can be because when a Darknet market gets taken down, law enforcement agencies are more focused on arresting vendors then they are arresting buyers. Furthermore, selling drugs is generally considered to be a more serious crime than merely possessing or using drugs, leading to a potentially greater negative outcome for buyers than for vendors.

A Darknet market shutdown can also have dramatic effects on the trust relations between a vendor and their customer base. A vendor identifies themselves by their PGP key, which is tied to their online identity. Verifying this key allows other users to ensure that a vendor is actually whom they say they are. While a Darknet market getting shut down does not lead to their PGP keys getting compromised, it can lead to some vendors becoming afraid of their real-life identity being revealed. After the Hansa takedown, some vendors completely changed their identity, including creating new PGP keys. This means that all their previous customers can now no longer distinguish them from all other vendors. One vendor had this as his main concern:

> *"After Hansa got shut down I burned my keys so I had to start all over again. After that I improved my opsec so now the biggest thing that would happen would be me losing the money held in escrow from sent packets. But most markets exitscam[sic] anyway so that can always happen."*

Losing their identity means that all the trust they had built up with their customers was lost in an instant. Such a loss can be devastating to their business, especially if their Darknet market activities were their only source of income.

Overall impressions on vendor behaviour

The greater concern about their privacy compared to the relative lack of it that was seen in the buyer cohort is most likely due to the increased risk buyers can experience after a Darknet market shutdown. Buyers merely risk losing money and the remote risk of arrest, but big vendors on a Darknet market risk being arrested and incarcerated. Vendors also risk losing their major source of income beyond the chance of getting arrested. Vendors have more to lose when their identities are revealed. as such, they have bigger concerns when their usage logs fall into the hands of the authorities.

Vendors, like buyers, also prefer mechanisms that allow them to create bonds of trusts between themselves and their buyers. Reviews and comments especially are seen as especially important, with some vendors even refusing to do any further business with buyers that left a negative review without first discussing it with them. Unlike buyers, they seem to have a more positive view of Darknet markets themselves. This could be because they have more regular contact with Darknet market administrators and have a better view of what happens "under the hood", so to speak, thereby trusting them more than buyers would, for whom the Darknet market administrators are a mostly unknown group.

4.2.5 Willingness to participate in a further interview

A section asking whether respondents were willing to participate in a further interview was present, but no respondent was willing to participate.

4.3 Research question discussion

From observing the results, we have distinguished two main types of trust-building mechanisms. Here defined as technological trust mechanisms, and organic trust mechanisms. A further explanation for these can be found in chapter 2.

Users overwhelmingly seem to prefer organic trust mechanisms over technological trust mechanisms. The survey results showed that mechanisms such as feedback systems and comment systems were the most highly valued, while technological trust mechanisms are either considered irrelevant or untrustworthy. The qualitative answers from the majority of respondents seem to indicate that users expect that market can be shut down due to law enforcement takedowns or exit scams at any time, and seem to believe that exit scams, in particular, are a threat to them.

Because of this, mechanisms that primarily try to create trust between a user and a market platform are considered to be of less value, as users believe that trust to be inherently transitory.

Organic trust mechanisms, on the other hand, are valued more highly as it allows users to create lasting bonds of trust between each other that can be transferred over to other market platforms.

Not all technological trust mechanisms are considered unimportant, however. Mechanisms such as encrypted private messaging, which allows market platform users to exchange encrypted messages with each other, are considered to be very important as well.

When it comes to changes in user behaviour among buyers after a market platform shutdown, the respondents seemed apathetic about any law enforcement agencies contacting them, and were more worried about losing money from interrupted transactions. Market shutdowns also did not seem to stop users from interacting with other market platforms, as traffic on the remaining market platforms increased after the shutdowns.

Vendors were more worried about market shutdowns, as the selling of drugs generally carries a higher sentence and comes with more law enforcement attention than merely buying them. But even so, "veteran" vendors, those that have experienced multiple shutdowns, did not seem worried about being caught after a shutdown; believing they have hidden their personal information well enough such that no law enforcement agency would be able to track them.

According to the results of the LDA model, the vast majority of profiles and listings seem to come from the Western nations and the Anglosphere. These nations include the US, Canada, the EU, and Australia. There can be several reasons for this. One of the reasons could be that the legal systems in these countries have lower legal punishments than other nations. Being convicted for trading in drugs might be punished with a fine and a prison sentence in the previously mentioned countries, while a similar act could be punishable by death in other nations such as Singapore or China.

Furthermore, access to Tor is also easier in Western nations. Tor is freely accessible in these nations, while its use and functionality is severely constrained or even criminalized in some nations, further increasing the barrier to entry to the online drug trade, both as a buyer or as a vendor.

From the respondents of the survey, the cohort was overwhelmingly male, with only a single female respondent, and was primarily composed of young adults, with the majority being younger than 30 years old. Looking at the types of drugs that were available at the Darknet markets, it seems that the majority of purchases were "soft" drugs such as Cannabis and LSD, along with pharmaceuticals. "Hard" drugs such as Heroin or Cocaine were not quite as common.

Chapter 5

Conclusions

The purpose of this thesis was to research how vendors and buyers manage to create positive transaction relations and the mechanisms they use in order to establish trust between each other. A secondary objective was to find which various kinds of trust mechanisms exist in cryptomarkets and how these specific mechanisms help to achieve establishing trust. This was done through the creation of a survey which was distributed to various Darknet communities and individual Darknet users. Through the qualitative answers gained from this survey, we can draw some conclusions on how trust is established and through what means.

5.1 Research findings

Two main types of trust-building mechanisms were distinguished. Technological trust mechanisms and organic trust mechanisms. Both users and vendors seemed to greatly prefer using organic trust mechanisms over technological trust mechanisms as it allowed users to create direct bonds of trust between each other, and those bonds were also irrespective of the market platform that they were created on.

Users are generally suspicious of market platforms, as they expect them to either get taken down by law enforcement or perpetrating an exit scam. Therefore, mechanisms that serve to increase trust between users and market platforms are not valued.

5.2 Study limitations

The group that was sampled was limited in scope, only including Darknet users, and only those visiting specific communities or market platforms. As such, making generalizations about the entire Darknet community and especially the general population from the results gathered in this thesis is not recommended. This is furthered by the low amount of responses, which means it is not possible to draw quantitative conclusions from the results. This is most likely because the part of the general population that was approached was already very small, and because the survey questioned people about inherently illegal behaviour, making people more hesitant to respond.

The survey also lacked a qualitative question related to general market platform selection, meaning that there were no decent qualitative answers available for that specific aspect of Darknet user behaviour. Therefore, the answer to that question could only be inferred from related survey questions and very broad market statistics instead of qualitative answers.

Market administrators were also not approached when distributing the survey. While that group is much smaller than even the group of active vendors, market administrators and moderators could have offered a unique perspective on the actions taken by market platforms when implementing certain mechanisms and how markets themselves deal with shocks to the whole cryptomarket ecosystem and the damage exit scams do to trust within the community.

5.3 Future work

While this thesis has attempted to answer some general questions about the mechanisms of creating trust in Darknet market platforms, the initial scope of the survey was too constrained. The scope was limited to how trust was created on the market platforms themselves and not in other locations such as forums or other types of message boards, locations where a lot of interaction between buyers and sellers takes place and which is used by both parties. The vendors use them to market themselves and reach a wider audience, and the buyers use such forums to gather information and reviews about vendors. On forums such as the Hub, Envoy forum, and Dread, vendors create threads to market themselves and to state how they can be reached and on what markets they are active. Buyers also post threads asking other buyers whether a certain vendor can be trusted, or what their general experience with specific market platforms is.

Therefore, a further study which takes a broader view and takes the entire spectrum of Darknet communities into consideration could offer a more complete overview on how cryptomarket users engage with each other and how they establish trust, as free-wheeling discussion platforms can be more appropriate for such a purpose than a market platform dedicated primarily to facilitating anonymous drug transactions.

Bibliography

[1] Deepdotweb - surfacing the news from the deep web. https://www.deepdotweb.com/. Accessed: 2018-02-09. 6

[2] Fbi arrests alleged 'silk road 2.0' operator blake benthall. NBC News, 2013. https://www.nbcnews.com/tech/security/fbi-arrests-alleged-silk-road-2-0-operator-blake-benthall-n242751. 7

[3] Cryptonote - the next generation cryptocurrency. DeepDotWeb, 2019. https://cryptonote.org/. 7, 38

[4] How direct deposit (wallet-less escrow) works. https://bntee6mf5w2okbpxdxheq7bk36yfmwithltxubliyvum6wlrrxzn72id.onion.ws/dd, 2019. 11

[5] Judith Aldridge and David Décary-Hétu. Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, 35:7–15, 2016. 1, 5

[6] 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. 5

[7] Michael K Bergman. White paper: the deep web: surfacing hidden value. *Journal of electronic publishing*, 7(1), 2001. 3

[8] David M Blei, Andrew Y Ng, and Michael I Jordan. Latent dirichlet allocation. *Journal of machine Learning research*, 3(Jan):993–1022, 2003. 16

[9] Michael A Brown Sr and Leigh Hersey. Returning to interpersonal dialogue and understanding human communication in the digital age. IGI Global, 2018. 4

[10] Paul Chiasson. Rcmp warns dark web being used to sell illicit guns to canadians. The Canadian Press, 2018. https://www.theglobeandmail.com/canada/article-rcmp-warns-dark-web-being-used-to-sell-illicit-guns-to-canadians/. 8, 39

[11] Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, and Martin Rösler. Below the surface: Exploring the deep web. *Trend Micro*, pages 1–48, 2015. 4, 5

[12] Catalin Cimpanu. Russia passes bill banning proxies, tor, and vpns. BleepingComputer, 2017. https://www.bleepingcomputer.com/news/government/russia-passes-bill-banning-proxies-tor-and-vpns/. 3

[13] Catalin Cimpanu. Another dark web marketplace bites the dust – wall street market. ZD Net, 2019. https://www.zdnet.com/article/another-dark-web-marketplace-bites-the-dust-wall-street-market/. 7, 8, 38

[14] C.M. Why you should never finalize early (fe). DarkWebNews, 2018. https://darkwebnews.com/scams/why-you-should-never-finalize-early-fe/. 11

[15] Devin Coldewey. How german and us authorities took down the owners of darknet drug emporium wall street market. techcrunch, 2019. https://techcrunch.com/2019/05/03/how-german-and-us-authorities-took-down-the-owners-of-darknet-drug-emporium-wall-street-mark 8, 10, 38

[16] Derek B Cornish and Ronald V Clarke. *The reasoning criminal: Rational choice perspectives on offending*. Transaction Publishers, 2014. 12

[17] Joseph Cox. 'silk road reloaded' just launched on a network more secret than tor. Motherboard, 2015. https://motherboard.vice.com/en_us/article/wnj449/silk-road-reloaded-i2p. 7

[18] DeepDotWeb. Blackbank market now offering multisig escrow. DeepDotWeb, 2014. https://www.deepdotweb.com/2014/02/16/blackbank-market-now-offering-multisig-escrow/. 11

[19] A. Evangelista. Darknet markets - competitive strategies in the underground of illicit goods. Eindhoven University of Technology, 2018. 13, 14

[20] European Monitoring Centre for Drugs and Drug Addiction. Drugs and the darknet perspectives for enforcement, research and policy. Europol, 2017. 6

[21] Lorenzo Franceschi-Bicchierai. Iran is trying to block tor. Motherboard, 2015. https://motherboard.vice.com/en_us/article/ae3am5/iran-is-trying-to-block-tor. 3

[22] Amrutha Gayathri. From marijuana to lsd, now illegal drugs delivered on your doorstep. International Business Times, 2011. https://www.ibtimes.com/marijuana-lsd-now-illegal-drugs-delivered-your-doorstep-290021. 6

[23] Andy Greenberg. Operation bayonet: Inside the sting that hijacked an entire dark web drug market. https://www.wired.com/story/hansa-dutch-police-sting-operation/, 2018. 3, 7

[24] Baldur Jón Gústafsson et al. *Darknet Market Usage Among Swedish Residents*. PhD thesis, 2016. 11

[25] Alice Hutchings. *Theory and Crime: Does it Compute?* Griffith University, 2013. 13

[26] Alice Hutchings and Richard Clayton. Exploring the provision of online booter services. *Deviant Behavior*, 37(10):1163–1178, 2016. 13

[27] Charles Arthur James Ball and Adam Gabbatt. Fbi claims largest bitcoin seizure after arrest of alleged silk road founder. The Guardian, 2013. https://www.theguardian.com/technology/2013/oct/02/alleged-silk-road-website-founder-arrested-bitcoin. 7

[28] Swati Khandelwal. Dark web users suspect "dream market" has also been backdoored by feds. The Hacker News, 2017. https://thehackernews.com/2017/07/dream-market-darkweb.html. 37

[29] James Martin. Lost on the silk road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice*, 14(3):351–367, 2014. 1

[30] Chris McCandless. Scam prevention and finalizing early. DeepDotWeb, 2015. https://www.deepdotweb.com/2015/10/30/scam-prevention-and-finalizing-early/. 11

[31] Urszula McCormack and Jack Nelson. Spotlight on the dark net: what does the alphabay takedown mean for you? KWM, 2017. https://www.kwm.com/en/hk/knowledge/insights/spotlight-on-the-dark-net-alphabday-takedown-20170727. 10

[32] Samuel C McQuade. *Understanding and managing cybercrime*. Pearson/Allyn and Bacon Boston, 2006. 13

[33] Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, et al. An empirical analysis of traceability in the monero blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018(3):143–163, 2018. 7, 38

[34] National Institute on Drug Abuse. Illicit drug use in the united states. https://d14rmgtrwzf5a.cloudfront.net/sites/default/files/past-month-use-by-age-2012-and-2013.gif, 2013. 24

[35] Gareth Owen and Nick Savage. The tor dark net. 2015. 3

[36] Nathaniel Popper. Alphabay, biggest online drug bazaar, goes dark, and questions swirl. The New York Times, 2017. https://www.nytimes.com/2017/07/06/business/dealbook/alphabay-online-drug-bazaar-goes-dark.html. 7

[37] Nathaniel Popper and Rebecca R. Ruiz. 2 leading online black markets are shut down by authorities. https://www.nytimes.com/2017/07/20/business/dealbook/alphabay-dark-web-opioids.html, 2017. 3

[38] Rob Price. We spoke to the shady opportunist behind silk road 3.0. The Daily Dot, 2013. https://www.dailydot.com/layer8/silk-road-3-blake-benthall/. 7

[39] Jamie Redman. Berlusconi admins disappear — darknet users rush to find alternatives. https://news.bitcoin.com/berlusconi-market-admins-disappear-darknet-users-rush-to-find-alternatives/, 2019. 8

[40] 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. 1

[41] Rolf Van Wegberg, Samaneh Tajalizadehkhoob, Kyle Soska, Ugur Akyazi, Carlos Hernandez Ganan, Bram Klievink, Nicolas Christin, and Michel Van Eeten. Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 1009–1026, 2018. 5

[42] Rolf van Wegberg and Thijmen Verburgh. Lost in the dream? measuring the effects of operation bayonet on vendors migrating to dream market. In *Proceedings of the Evolution of the Darknet Workshop*, pages 1–5, 2018. 1

[43] Daniël Verlaan. Politie brengt 37 kopers van drugs op darkweb een bezoekje. https://www.rtlnieuws.nl/technieuws/artikel/3858331/politie-brengt-37-kopers-van-drugs-op-darkweb-een-bezoekje, 2018. 27

[44] Philipp Winter and Stefan Lindskog. How china is blocking tor. Cornell University, 2012. https://arxiv.org/abs/1204.0447. 3

[45] Nicky Woolf. Bitcoin 'exit scam': deep-web market operators disappear with $12m. The Guardian, 2015. https://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars. 10

Appendix A

Appendix

A.1 Further description of reviewed markets

A.1.1 Dream Market

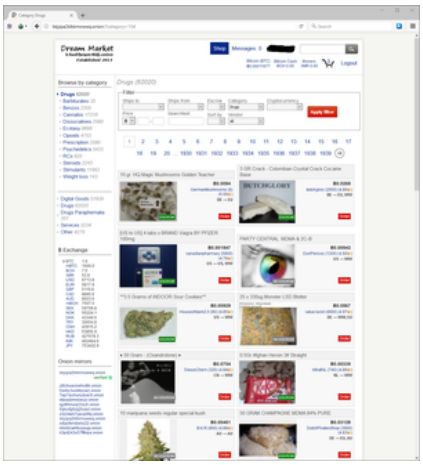

Figure A.1: Image of Dream market's front page

Before the shutdown of Hansa and AlphaBay, Dream Market was the second largest Darknet market platform, with AlphaBay being the largest and Hansa the third largest. After the shutdown of Hansa and AlphaBay, many speculated that Dream Market would swiftly see an increase in users as people from the other two platforms would flock to Dream Market. From looking at the statistics, this seems to have been the case. Although it has not yet reached the size that AlphaBay once had, with over 369,000 listings and 400,000 users, Dream Market's number of listing went from around 61,000 listings in July 2017 [28] to over 166,000 listings in February 2019, making Dream Market the largest market platform currently online. Dream Market was started in 2013, making it the oldest market of the three.

Dream Market offers an escrow service, but also allows for finalize early transactions for verified and trusted vendors. Dream Market also operates a separate forum where vendors, buyers and staff members can interact. Besides Bitcoin, which all three markets accept, Dream Market also accepts Bitcoin Cash.

Dream Market also possesses all the features common to modern market platforms such as features customer reviews, vendor ratings and other information which is used to decrease the information gap between vendor and buyer.

A.1.2 Wall Street Market

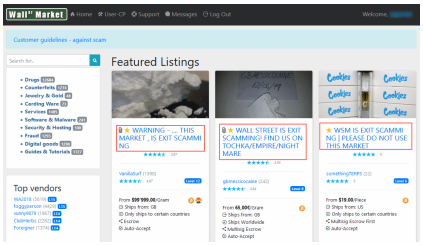

Figure A.2: Image of Wall Street Market's front page. Note the renamed listings warning users of a suspected exit scam [13]

Only launched in 2016, Wall Street Market is the newest market platform covered in this thesis. Perhaps due to its young age it attempts to be a more modern iteration of a Darknet market platform. It is the only market discussed here that accepts Monero, something Alphabay was known for shortly before it was shut down. Monero is a cryptocurrency based on the Cryptonote [3] protocol, which allows users to obscure the transaction graph by including chaff transactions called "mixins", while Bitcoin explicitly shows the complete, unaltered transaction graph. This allows users to spend their currency with increased privacy[33]. It also offers multisig support, beyond all the "standard" features (review system, rating system).

In mid April, users of Wall Street Market noticed that they could no longer withdraw money from the escrow wallets used by the market. Initially, the administrators told users that this was a temporary connection issue, and that the administrators had temporarily moved the funds to another wallet until the issue was resolved. Users were unimpressed with this explanation, and accused the administrators of perpetrating an exit scam[13]. The traffic generated by this event drew the attention of German and American law enforcement agencies, who took advantage of the chaotic situation to track down the main operators of the market[15].

A.1.3 Tochka Free Market

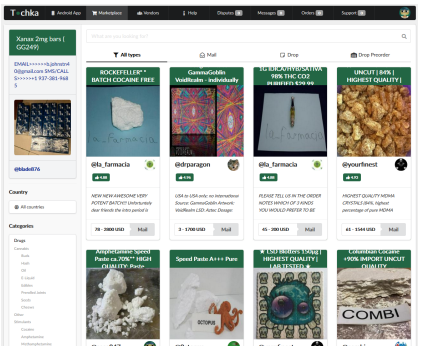

Figure A.3: Image of Tochka's interface

Tochka Free Market, also know as T.chka or the Point, is the smallest market reviewed in this thesis. Possibly due to its policy of not offering an escrow service and thereby offering a less trustworthy purchase experience of other markets. It does offer a service not offered by other market platforms, however. Tochka offers the possibility of setting up dead drops, a secret location that is used to transfer items. This method allows both buyers and vendors to make a transaction while remaining anonymous and without employing the postal service, in which a parcel could be more easily intercepted by law enforcement agencies.

A.1.4 Berlusconi Market

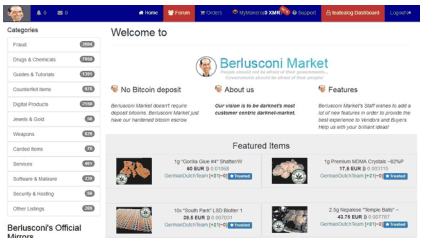

Figure A.4: Image of Berlusconi market's interface

Named after the former prime minister of Italy, Silvio Berlusconi, Berlusconi market is a fast growing traditional escrow market and one of the few remaining larger markets currently extant in the darknet ecosystem. The amount of listings especially increased after the shutdown of Dream Market and Wall Street Market, with the number of drug listings almost doubling since the shutdown of Wall Street Market to 28,500 listings.

Until recently, Berlusconi was also one of the few markets to have weapons as part of its catalogue. While other markets might sell weapons such as tasers, or perhaps ammunition for 9 millimeter weapons, Berlusconi offered long guns such as AK47's or M16 style platforms[10].

A.1.5 Empire Market

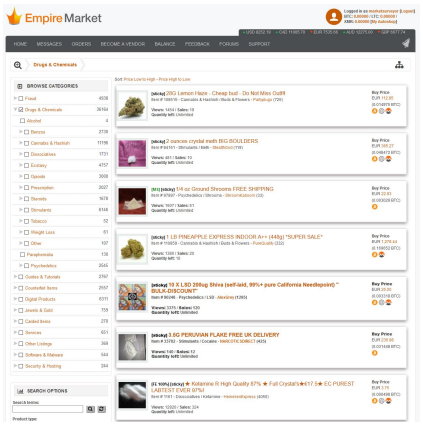

Figure A.5: Image of Empire market's interface

Empire market is one of two remaining extant darknet markets. Being slightly larger than Berlusconi, with 36,000 drug listings, it has also experienced a period of growth after the shutdown of its competitors.

Empire market is a standard escrow market, most reminiscent of the defunct AlphaBay in its UI design. It offers multisig escrow, 2-factor authentication and accepts multiple different forms of cryptocurrency, those being bitcoin, LiteCoin and Monero.

A.1.6 Cryptonia

Cryptonia is a fairly recently created market and whose design was created as a response to the various darknet markets that have exit scammed or had their Bitcoin wallets compromised in other means. It's main feature is a wallet-less escrow system. Instead of Cryptonia itself having a wallet in which users deposit coins used for trading goods, a single-use wallet is created for each

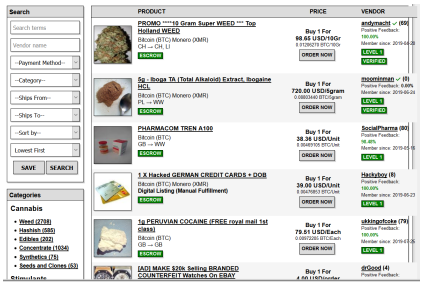

Figure A.6: Image of Cryptonia's interface

individual purchase that only the vendor and buyer have access to. The market itself has no way of accessing the funds in such an account, giving the administrators less opportunity to steal the deposit or have the deposit stolen by a hacker if they were to compromise the market's servers. The fee for the market is also randomized between 2% and 4% of the price, in order to prevent blockchain analysis attacks.

A.2 Survey

Section 1: Cryptomarkets - General

This section contains question related to your general engagement with cryptomarkets

1: Which of the following cryptomarkets are you currently participating in?

2: How did you first learn of the cryptomarkets you are participating in?

3: Which of the following (now offline) cryptomarkes have you participated in?

4: Were you still participating in these markets before they were shut down? If no, could you please tell us why you stopped using them?

5: Have the recent shutdowns of Dream Market and Wall Street Market impacted your cryptomarket usage? If so, how?

6: How much time do you spend on cryptomarkets on a daily basis?

7: (This question is mandatory)
On your chosen cryptomarket(s), are you primarily a vendor or a buyer?

Section 2: Cryptomarkets - Buyer (Only viewable if "Buyer" or "Both" was selected in question 7)

8: How important do you consider the following aspects when choosing on which cryptomarket(s) you will purchase items?

- Large amount of vendors and listings
- Responsiveness/competence of the administration team
- Webstore functionalities (E.G. product categories)
- Privacy Measures (E.G. encrypted private messaging)

9: How important do you consider the following aspects to making a specific purchase?

- Large amount of comments
- High fraction of positive comments
- You have previously successfully purchased a product from the same vendor
- The vendor's profile and listing page
- Price to perceived quality ratio
- Secure and private shipping options
- Finalize Early
- 2 out of 3 multisig
- Walletless Escrow

10: If the cryptomarket(s) you are currently operating on were shut down by authorities, what would be your biggest concern as a buyer?

Section 3: Cryptomarkets - Vendor (Only viewable if "Vendor" or "Both" was selected in question 7)

12: Are your cryptomarket activities your primary means of income?

13: What is the monthly income from your cryptomarket activities?

14: What are the nation(s) you ship from?

15: What are the nation(s) you ship to?

16: How important do you consider the following aspects to your decision to start selling on your chosen cryptomarket(s)?

- The market isn't saturated by too many vendors
- Responsiveness/competence of the administration team
- The number of potential buyers
- Webstore functionalities (E.G. product categories)
- Privacy measures (E.G. encrypted private messaging)

17: How important do you consider the following aspects of cryptomarkets to your ongoing business?

- Review System (The ability to star review the product)
- Feedback system (The ability to add comments to a product)
- Acceptance of coins other than Bitcoin
- Finalize Early
- Standard Escrow
- 2 out of 3 multisig
- Transaction security
- Marketplace anti-phishing features

19: If the cryptomarket(s) you are currently operating on were shut down by authorities, what would be your biggest concern as a vendor?

Section 4: General Questions

20: What is your gender?

21: What is your age?

22: How experienced would you rate yourself when it comes to digital security compared to the general population?

23: What is the highest educational degree you have completed?

Section 5: Further participation

Thank you very much for taking the time to answer questions about your cryptomarket usage. We really hope you are willing to contribute to an anonymous follow-up interview to further discuss your cryptomarket habits. If you do not wish to participate, please leave this section blank.

24: Would you be willing to participate in a follow-up interview on an anonymous channel?

25: What is the method of communication we can use to reach you for a further interview?

26: How can we reach you at the indicated method of communicated (ID/username)? We will soon get in touch with you to set up a time at your best convenience. Thank you!