

ECONOMICS OF ILLICIT BEHAVIORS:
EXCHANGE IN THE INTERNET WILD WEST

by

Julia R. Norgaard
A Dissertation
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
The Requirements for the Degree
of
Doctor of Philosophy
Economics

Committee:

_____ Director

_____ Department Chairperson

_____ Program Director

_____ Dean, College of Humanities
and Social Sciences

Date: _____ Spring Semester 2017
George Mason University
Fairfax, VA

Economics of Illicit Behaviors: Exchange in the Internet Wild West

A dissertation submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy at George Mason University

By

Julia R. Norgaard
Master of Arts
George Mason University, 2015
Bachelor of Arts
University of San Diego, 2012

Director: Dr. Thomas Stratmann, Professor and Dissertation Chair
Department of Economics

Spring Semester 2017
George Mason University
Fairfax, VA

Copyright 2017 Julia R. Norgaard
All Rights Reserved

Dedication

This is dedicated to my wonderful parents Clark and Jill, who introduced me to economics and taught me how to be a dedicated scholar and a good and faithful person.

Acknowledgements

Thank you to my family and friends who have supported me throughout my graduate journey. My boyfriend, Ennio, who gave me feedback on my research and provided helpful comments and encouragement. My colleagues who have provided me with fruitful discussion, endless support, and wonderful friendship. My committee who has provided me with invaluable help and guidance.

Table of Contents

	Page
List of Tables.....	xi
List of Figures	xii
Abstract	ix
<u>Chapter 1</u>	1
1. Introduction.....	1
2. An Overview of the Deep Web.....	4
3. Reputation as a Mechanism for Market Accountability.....	8
4. Theoretical and Empirical Model.....	12
5. Empirical Model	20
6. Data from the Silk Road.....	21
Data Collection Procedure.....	22
Variables Used in Empirical Analysis.....	24
7. Results.....	26
Estimating Beta.....	29
8. Conclusion.....	31
<u>Chapter 2</u>	34
1. Introduction.....	34
2. The Dark Net.....	37
3. The Economics of Anonymity, Private Governance, and Club Goods.....	40
Anonymity.....	40
Private Governance and Club Goods.....	44
4. A Model of the Internet Black Market.....	46
The Anonymity Problem.....	46
5. Evidence.....	50
Private Governance in The Dark Net.....	50
Residual Claimancy.....	52
Exclusion.....	54
Advertising.....	55
Branding.....	57
Contract Enforcement.....	59
Fraud Prevention.....	60
Provision of Club Goods in the Dark Net.....	62
Personal Security Services.....	62
Conflict Resolution Services.....	65
6. Conclusion.....	67
<u>Chapter 3</u>	69

1. Introduction.....	69
2. The Digital Marketplace for Illicit Goods.....	71
The Dark Net.....	71
Tor: The Onion Router.....	72
Cryptomarkets.....	73
3. Markets and Hierarchies.....	76
Organized Crime.....	76
Networks and Hierarchy.....	80
Hypothesis.....	82
Preliminary Evidence.....	82
4. Testing our Hypothesis Using Agent Based Modeling.....	83
Purpose.....	83
The Mechanics of Agent Based Modeling.....	85
Our Model.....	88
Model Visuals.....	91
Entities, State Variables, and Scales.....	96
Process Overview and Scheduling.....	99
Process Overview of Ground Model.....	100
Process Overview of Virtual Model.....	101
Design Concepts.....	102
Results.....	105
5. Conclusion.....	116
Appendix.....	118
List of References.....	136
Biography.....	148

List of Tables

Table	Page
1. Summary Stats	26
2. GLS Regressions of Effect of Reputation on Log Price per Gram.....	28
3. β	30
4. Unedited List of Drug Types Parsed from Dark Web Data.....	Appendix

List of Figures

Figure	Page
1. Darknet Markets 1	Appendix
2. Darknet Markets 2.....	Appendix
3. Silk Road 1.....	Appendix
4. Silk Road 2.....	Appendix
5. Feedback.....	Appendix
6. Item View.....	Appendix
7. Initial Scenario	47
8. Provision of Private Governance and Club Goods.....	49
9. Darknet Market Lifespan	Appendix
10. Support.....	Appendix
11. Product on Dream Market.....	Appendix
12. Product on AlphaBay.....	Appendix
13. Listing Feedback on AlphaBay.....	Appendix
14. Listing Feedback on Wall St. Market.....	Appendix
15. Forums Hansa 1.....	Appendix
16. Forums Hansa 2.....	Appendix
17. Hansa Top Vendors.....	Appendix
18. Wall St. Market Featured Listings.....	Appendix
19. Hansa Drugs.....	Appendix
20. All Products on Valhalla.....	Appendix
21. Free Sample Hansa.....	Appendix
22. Dream Market Forums 1.....	Appendix
23. Dream Market Forums 2.....	Appendix
24. Shop Dream Market.....	Appendix
25. Remove Feedback.....	Appendix
26. PGP 1.....	Appendix
27. PGP 2.....	Appendix
28. Forbidden Goods on Hansa.....	Appendix
29. Hansa Knowledge Base and Support.....	Appendix
30. Vendors.....	Appendix
31. To Setup.....	Appendix
32. Decide to Buy More Drugs Virtual 1.....	Appendix
33. Decide to Buy More Drugs Ground 1.....	Appendix
34. Turtles.....	Appendix
35. To Setup 2.....	Appendix

36. Set up Agents.....	Appendix
37. Decide to Buy More Drugs Virtual 2.....	Appendix
38. Decide to Buy More Drugs Ground 2.....	Appendix
39. Controller Setup for Virtual Network.....	91
40. Model Outcomes.....	92
41. Output and Layout.....	93
42. Output Ground Network.....	94
43. Network Connections Ground Network.....	95
44. Network Connections Ground Network Layout.....	95
45. Network structure of Virtual network (Average Degree: 2.03, Density: 0.014).....	106
46. Network structure of Ground network (Average Degree: 1.17, Density: 0.008).....	106
47. Average Path Length in Virtual and Ground Networks after 100 runs.....	108
48. Average Degree in Virtual and Ground Networks after 100 runs.....	111
49. Average Betweenness in Virtual and Ground Networks after 100 runs.....	112
50. Average Network Density in Virtual and Ground Networks after 100 runs.....	112
51. Average number of “strong” clusters in Virtual and Ground Networks.....	114
52. Average number of “weak” clusters in Virtual and Ground Networks.....	114
53. Average Percent of Possible Transactions in Virtual and Ground Models.....	115

Abstract

ECONOMICS OF ILLICIT BEHAVIORS: EXCHANGE IN THE INTERNET WILD WEST

Julia R. Norgaard, Ph.D.

George Mason University, 2017

Dissertation Director: Dr. Thomas Stratmann

The first paper is an analysis of the role reputation plays in the Deep Web using data from the Internet black market site, The Silk Road. This encrypted online marketplace employed crypto currency and functioned over the Tor network. Utilizing a modeling technique, informed by trade auction theory, we investigate the effect of seller reputation. Analysis of the seller's reputation gives us insights into the factors that determine the prices of goods and services in this black marketplace. Data on cannabis listings is parsed from the Silk Road website and covers an 11-month time period, from November 2013 to October 2014. This data demonstrates that reputation acts as a sufficient self-enforcement mechanism to allow transactions. These findings exemplify the robustness of spontaneous order with respect to the Deep Web as an emergent marketplace.

The second paper examines how the platform providers in the Internet Black Market, one of the world's largest international markets for illicit goods and services,

allow buyers and sellers to overcome the problems anonymity poses to exchange. These online markets enable users to repeatedly exchange in an environment with no third party enforcement while keeping their identity concealed from law enforcement.

The third paper analyzes the determinants of network structure, as measured by hierarchy and monopolization, by examining various black market networks. We examine structures of networks in the Internet Dark Net (virtual) and compare it to network structures of traditional black markets (ground), using agent-based modeling. The purpose of modeling these two different types of illicit markets is to understand the network structure that emerges from the interactions of the agents in each environment. Traditional black markets are relatively hierarchical, with high degree and high betweenness. We compare the density and average length of shortest path of the simulated ground black market networks with our simulated virtual network. We find that hierarchy and monopolization tendencies in networks are products of differences in transaction costs and information asymmetries. The Internet is an effective way to lower both of these aspects of network structure. We observe that the network structure surrounding the interactions in the virtual black market is less hierarchical and slightly more monopolistic than the network structure of the ground market.

Chapter 1: Reputation in the Internet Black Market: An Empirical and Theoretical Analysis of the Deep Web

1. Introduction

Modern black markets have in place numerous institutions to facilitate trade and evade law enforcement. Cash makes transactions untraceable, hierarchy delineates roles and responsibilities, and violence encourages participants to abide by norms. The advent of the Internet razes this system; entirely new institutions are required for black market trades in this environment. The increased anonymity lowers the risk of detection by law enforcement (LE) in exchange for an increase in the risk of impropriety between buyer and seller. This paper examines the use of seller ratings to facilitate trade through lower transaction and information costs.

Illegal Internet activities are conducted on a portion of the Internet referred to as the Deep Web, and is estimated to be thousands of times larger than the Surface Web, the Internet we use every day.¹ The Deep Web is unregulated, untaxed, and hidden from a typical Internet search. It is a self-contained market place that functions under a set of informal institutions. Using a representative data set mined from The Silk Road, one of the most popular sites on the Deep Web, we investigate the operation of these black-

¹ For a more detailed analysis of the Deep Web and surface web, see Chandler, 2013.

market transactions. We observe that the institution of seller reputations create a stable trading environment among those least expected to deal honestly: criminals.

Black market activity on the Deep Web is attractive because of the anonymity it provides. Cryptocurrencies such as Bitcoin function like cash; they are untraceable. The TOR network anonymizes web traffic. PGP encryption programs mask data within emails sent between users. These three elements form the technological base upon which Deep Web black markets build, allowing exchange at a much lower cost than previously. Before this technology, sellers and buyers in the black market relied heavily on face-to-face interaction and building a reputation through personal encounters. This shift led to a flourishing peer-to-peer underground marketplace expanding on a global scale.

But, anonymous Internet trading incurs an additional cost. Like buyers and sellers on any peer-to-peer Internet site such as eBay or Amazon, buyers and sellers on the Deep Web rarely, if ever, meet in person. This makes transactions particularly risky because there is no recourse for failure. And unlike goods on Surface Web sites, Deep Web users are buying products much more harmful than ordinary consumer purchases. The unique nature of this marketplace makes the accumulated reputation of users critical to its emergence and sustainability. Similar to Avner Greif's work on the Maghribi Traders, these Internet traders have asymmetric information (Greif, 1989). However, unlike the Maghribi Traders, these Internet traders have no legal contract enforceability (Skarbek, 2008). Analyzing this reputation component will enlighten, more fully, how this market place can exist without out any ability to seek recourse ex post and without any prevalence of contract enforceability (Greif, 2010). We empirically answer the

questions; does investment in reputation allow sellers to charge premium prices, or to simply remain in the market? How does reputation play a role in this marketplace?

The most important institution of the Deep Web is anonymity. Each buyer and seller is known by a unique username; their true identity is secret. Users of the Deep Web, through forums and blogs, create a wealth of information to keep users updated on the happenings of the market (DarkNet Markets, 2014). Figures 1-3 show Reddit's Deep Web forum and how the users communicate. They use these "news outlets" to keep users informed on frauds, scams, and imposters. Deep Web markets take a cut of each transaction to cover their operation costs and to make a profit. Buyers write and read extensive reviews on sellers and their products. Markets allow ratings from 0 to 5 stars, accompanied by a brief note explaining the rating. More extensive reviews are commonly posted on internal forums and Reddit. These jointly create the seller's reputation. Some sellers, to differentiate, offer free samples or extra secure shipping techniques to attract positive reviews.

This paper investigates a market place where feedback mechanisms and reputation are the only things keeping the market functioning, without any government taxation and regulation (Greif, 1989, Clay 1997). Deep Web markets are an empirical example of the depth of robustness of spontaneous order. It shows that the principles of an unfettered market rooted in reputation and accountability can be applied to an extremely vast array of goods and services. We are fundamentally analyzing how individuals interact with each other and without government (Powell & Stringham, 2009; Leeson, 2010). In section 2 we delve into the factors that differentiate the Deep Web

from other online marketplaces. Section 3 explores how reputation provides a market mechanism to keep buyers and sellers accountable and honest. We outline and describe our theoretical model in section 4, analyzing how reputation functions in the market. Our empirical method of analysis is laid out in section 5. Section 6 includes a description of our data, our collection procedure, and detailed definitions of all our variables. Section 7 reviews our results and estimates the buyers' and sellers' discount factors. Our concluding remarks about the implications and impact of our findings are enclosed in section 8.

2. An Overview of the Deep Web: What Differentiates it from Other Online Marketplaces

The currency used to make transactions in the Deep Web is Bitcoin. A Bitcoin is a solution to a mathematical equation, and a pseudo-anonymous crypto currency (Grinberg, 2011). They are stored in virtual wallets and are exchanged through anonymous virtual transactions with low transaction fees (Briere, 2013). To "mine" Bitcoins, "miners" use computing power to solve mathematical problems to which there are a fixed number of solutions. Because of the fixed nature of the number of possible solutions (Bitcoins), this crypto currency, by design, cannot be inflated. Therefore, this alternative currency is free from central bank policies or intervention (ECB, 2012).

According to Nicolas Christin, in his paper *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*, "Bitcoin is a peer-to-peer, distributed payment system that offers its participants to engage in verifiable transactions without the need for a central third-party" (Christin, 2012). Bitcoins are

used for Deep Web transactions because they are anonymous, like cash, and can be transacted electronically. A Bitcoin wallet functions like a physical wallet with cash: once you transfer Bitcoins from one wallet to another, it is untraceable and permanent.

The Deep Web exists on Tor, a computer networking system that allows for anonymous communication and transactions. The communications sent on Tor are encrypted and then sent through numerous network servers and nodes. When users communicate through the Surface Web their messages are unencrypted and travel directly from sender to receiver. Messages are ‘bounced’ between nodes in the Tor network, making them virtually untraceable. The random path the message takes, coupled with its encryption while traveling through the network secures the anonymity of the users and security of the content. This message ‘bouncing’ cause the Tor network to be much slower than Surface Web networks. The identity of the sender and receiver of a message over Tor is hidden unless the user explicitly wishes to reveal their identity (Onion Routing, 2014). Because Bitcoin is an anonymous crypto currency, it is used as a medium of exchange on Tor.

The barriers to entry into the deep web are very high. The use and knowledge of Bitcoin takes some degree of computer sophistication. However, Bitcoins are becoming increasingly popular and information about how to obtain and use them is readily available. The use and implementation of Tor, on the other hand, suffers from a very large knowledge problem. Jeffrey Tucker, founder of Liberty.me, describes the skills it takes to feasibly and securely make transactions over the Deep Web; “you have to be a sophisticated person to get into commercial buying and selling on the Silk Road”

(Tucker, 2014). Users thus turn to this type of market place because it provides them with goods and services more cheaply, more safely, or of a higher quality than their local black market would allow them to access. According to Tucker; “People have an intensity of demand to overcome technical barriers” because there are no online tutorials and much of what goes on in Tor is illegal. There are also very high risk factors when it comes to anonymizing oneself, detection of one’s identity could result in stolen goods, personal safety issues, or imprisonment.

A primary difference between traditional online sites, such as eBay, and the Silk Road is escrow implementation. Standard escrow requires the ability to undo a transaction. Fraudulent items are returned to the seller, and then the escrow service refunds the buyer. Hu et al. preface their model on the assumption that “in the case of fraud, [escrow] users lose only the service fee” (Hu et al. 2004). Silk Road purchases cannot be undone; drug dealers don’t provide return addresses. An escrow service cannot exist which simultaneously satisfies buyer and seller.

The Deep Web is an untaxed and unregulated marketplace; it exists as a completely unfettered free-market. This marketplace functions much like the historical Law Merchant market did in medieval Europe and the medieval Maghribi Traders in the Mediterranean (Greif, 1989; Greif 2012). According to Benson;

the rules of property and contract necessary for a market economy, which most economists and legal scholars feel must be “imposed,” have evolved without the design of any absolute authority. Commerce and commercial law have developed conterminously, without the aid of and often despite the interferences of the

coercive power of nation-states because there is a mechanism in place (Benson 644-645)

With respect to the Silk Road, the ‘internal policing’ mechanism that Benson refers to is the reputation of sellers and buyers.

Because the users in this marketplace cannot seek legal recourse for their illegal transactions, they must police themselves (Milgrom, North, and Weingast, 2010). The Deep Web Culture promotes transparency with respect to the quality of the goods and services as well as honesty amongst buyers and sellers. Users have created checks and balances on each other to feel confident and safe on the Deep Web. Just like historical pirates (Leeson, 2007), buyers use checks and balances to constrain seller predation. In the absence of a central coercive force for recursive action, users must rely on each other for feedback and information. The security and reliability of this network is what keeps users confident in the marketplace because they provide internal checks on each other. Many forums contain information about people who are masquerading as prominent sellers, or users that are committing fraud. This emergent order is no surprise.

According to Peter Leeson, in his paper *Anarchy Unbound: How Much Order Can Spontaneous Order Create?* (2010), and Dennis Mueller in his paper *Anarchy, the Market, and the State* (1988), organization and structural norms emerge without the use of a central planner in the marketplace and these norms are effective at keeping users in the marketplace safe and satisfied with their services and products.

This marketplace has allowed for anonymous peer-to-peer engagement with only the Silk Road and other hosting sites to facilitate the exchange and take a small fee. In

their paper, *Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System*, Resnick and Zeckhauser (2001) stress that when there is repeated play among individuals in a marketplace it reduces the likelihood of dishonest people continuously dealing in the market and reduces moral hazard. This type of transaction has revolutionized the illegal goods and services trade because it has made it more convenient, accessible, and has allowed users to access a larger variety of the good of their choice. This online network has enabled local sellers of illegal goods to expand to a global setting, and increasing worldwide price and quality competition. In terms of the global drug market, the Silk Road is a small fraction. Kilmer and Pacula (2009) estimate a 2003 trade volume of \$142 billion. Court documents used in the trial of Silk Road Founder Ross Ulbricht (U.S. vs.) allege the original Silk Road grossed approximately \$214 million during its two years of operation.

The latest estimate of marijuana street prices comes from the Office of National Drug Control Policy (ONDCP). The ONDCP uses data from the National Survey on Drug Use and Health (NSDUH) to predict price per gram on the street. They find relatively stable prices, though the 2010 estimate of \$7.11/gram has declined from 2004's \$7.50/gram. They also extend the analysis to Fries et al. data set, estimating a 2010 street price of \$10.70/gram (Rand Corporation 2014; Fries et al. 2008). Our data set's median 2014 price of \$13.61/gram is consistent with a number of theories: higher quality marijuana, an Internet premium, or price inflation over the past four years. J.P. Morgan (2012) finds that revenue lost to online fraud is falling, estimated to 0.9% in 2011.

3. Reputation as a Mechanism for Market Accountability

Because of the nature of the goods sold in the Deep Web, on the Silk Road in particular, sellers are anonymous to buyers and buyers are anonymous to sellers. Before a first transaction, they have no personal knowledge of another's personality and no formal enforcement mechanism if a transaction goes awry. The characteristics of this particular marketplace pose risks to the traders involved. The buyer could refuse to pay the seller after their items have been received, or, if the buyer pays first, the seller could fail to send the purchased items because they received the payment upfront. There is no way to recoup lost Bitcoins or products once the transaction is finalized. This marketplace exists due to the importance of a bilateral reputation mechanism that instills confidence in the traders and facilitates repeated transactions (Greif, 2012).

In his paper *Endogenizing Fractionalization*, Peter Leeson (2005) makes the point that users “need to establish ex ante whether or not the outsiders they would like to trade with are ‘cheaters’ or ‘cooperators’”. In other words, they need a means of screening outsiders” (Leeson, 79). Collecting as much data as possible on the other party is necessary to making a smart and calculated transaction. Initially, buyers and sellers are dependent upon previous users' feedback for information on the legitimacy of their potential trade. Recognizing this potential risk, traders utilize forums such as Reddit and the Silk Road itself for feedback, bringing attention to fraudulent behavior and informing traders of transaction malfeasance.

The codification of buyer and seller feedback makes up each party's user profile (Houser and Wooders, 2006). A user's feedback profile in this marketplace is made up of the comments and ratings left on the Silk Road site as well as other feedback forums.

This feedback is both comments and a number rating. The collection of this user feedback on other users makes up the reputation of the trader in the marketplace. Due to the anonymity aspects of The Silk Road, buyer information is not formally posted like seller information and feedback is on the site. Unlike Surface Web marketplaces, if a buyer leaves a comment and/or rating, an individual identifier is not attached to their message. The reason for this is to protect buyer anonymity. The only information that we can glean about the buyer in particular is that they did in fact make a purchase; buyers cannot leave feedback on a product they did not buy.

Potential buyers utilize this feedback about sellers. They can read comments about previous buyer's experiences, whether or not the buyer received the items, and view the seller's 30-day and 60-day and overall rating score. This score is an average of past reviews and it is out of 5 possible points. Sellers, however, do not have access to this information about potential buyers. Repeated trade will reveal buyer reputation, but the first is made with little information. The promise of future trade can incentivize honest behavior from the beginning; sellers can cease trade with dishonest buyers.

Discovery of a dishonest buyer can have positive externalities for other sellers. But, sellers' outlets for relaying the information that they have learned from buyers are limited. Because buyers do not have publically available profiles, the seller must seek alternative forms of feedback. They can leave feedback on the internal Silk Road forums or various forums on the Surface Web, but cannot add to a collected reputation buyer profile because they do not exist. Gambetta, in his book "Codes of the Underworld: How Criminals Communicate", identifies that criminals need both a costly signal of the

trader's credentials and a costless arbitrary group signal in order for this type of market place to run smoothly underground (2010). Leeson (2005) further breaks down the components necessary for a successful reputation signal in general. He states that they must be easily observable and that they also must be costly for cheaters to signal a stellar reputation and fairly inexpensive for honest users to signal that they are authentic.

Applying these characteristics to the Silk Road marketplace, the seller feedback mechanisms of readily observable ratings, comments, and thus reputation fit these criteria and send a signal that the seller is honest or dishonest. It would be difficult for a repeatedly dishonest seller to trick its buyers to leave positive reviews and ratings even though the products and services were a sham. On the other hand, if an honest seller provides their customer's with quality products in a timely manner, it will be relatively easy to receive truthful positive reviews about the seller's quality performance. This dovetails very nicely with what we know about the Silk Road community from studying Silk Road forums: the community is very active at giving feedback. These criteria, easily observable signaling and costly signaling for cheaters, do not necessarily apply to the buyers in this marketplace. This failure of buyer feedback to meet the strong signal criteria proposes that buyer signals could contain a great deal of noise and potential for misread signals. For the purposes of this paper, we will analyze the impact of seller's reputation as a signal.

However imperfect these feedback mechanisms may be, they provide users information on reputation. Reputation is crucial in this market because it acts as a signal to other users that they are honest and credible individuals. This signal works to

differentiate between honest and dishonest users to ensure that honest users are not driven out of the marketplace by dishonest users that are not properly identified. Leeson (2005) emphasizes that the traders' identities work to reduce social distance in the marketplace. Deep Web traders do not have an identity in the traditional sense, however; they foster an identity through their online reputation. Leeson (2005) makes it clear that

cheaters, however, have higher discount rates than cooperators. This is in fact why they cheat. Because they discount the gains from future exchange more heavily than cooperators, cheaters find it relatively more costly to invest in creating some degree of homogeneity with an outsider, the value of which will only be recouped some time down the road. (Leeson, 80)

Our analysis in this paper estimates the discount factors of all users. An essential component to the reputation system is that, if reputation does allow sellers to charge their customers a premium, it behooves the sellers to increase their reputation so as to be able to collect premium profits. Therefore, the existence of the reputation system itself acts to ensure honesty with each transaction. This particular phenomenon is what this paper analyzes in great detail, whether or not an increase in reputation empirically and statistically significantly allows sellers to actually charge premium prices. We analyze if favorable reputation allows sellers to capitalize on their positive feedback and signal to buyers that their items are of high quality like Shapiro (1983) found in his paper *Premiums for High Quality Products as Returns to Reputation*.

4. Theoretical and Empirical Model

We seek to accomplish two goals. First, we disentangle the role of reputation on the Silk Road. Does investment in reputation allow sellers to charge premium prices, or to simply remain in the market? Houser and Wooders (2006) posit a market with *honest* and *dishonest* sellers. Reputation serves as a signal that a seller is honest. Thus, a buyer's utility, as well as willingness to pay, increases with increased seller reputation. This reputation enables sellers to earn a premium. Houser and Wooders find evidence supporting this theory using their data on eBay auctions. Other papers find similar results. Klein and Leffler (1981) examines the use of higher prices to ensure contractual performance, Shapiro (1983) as well as Allen (1984) examine prices above marginal cost to forestall quality cutting, and McDonald and Slawson (2000) examine returns to reputation in electronic auction markets.

Alternate theoretical models can be constructed such that reputation does not convey a premium. Rather, in equilibrium all sellers are *honest*. One could suppose that above a certain threshold a seller is considered *honest* by buyers and remains in the market, below that threshold the seller is considered *dishonest* and exits the market or creates a new identity. Melnik and Alm (2002) find some support for this theory. They show a positive relationship between reputation and price, but the predicted effect is quite small.

Second, what assumptions about time discounting must be made to sustain the market? Using the estimates of return to honesty, we can determine a lower bound to a seller's time preference. A seller with a higher time preference would be less patient for payment and would prefer the buyer to pay for the goods before they had received them.

This is called finalizing early (FE), and occurs when buyers transfer their payment in Bitcoins to the seller before the product is received. If the seller has a relatively low time preference, they would not necessarily request an FE payment. Not much work has been done on estimating this variable, though it has vast implications for the functioning of a market dependent upon repeated trade and weak punishments. FE was prevalent on the Silk Road prior to its shutdown. As markets have evolved, multi-signature escrow has become the norm.

We begin with a simple model, discussing the interaction between a single seller and buyer. We later expand this simple model's insight to a broader model. Choice nodes exist for buyers and sellers, each dependent upon the expectation of actions at the subsequent nodes. First we analyze the nodes chronologically and then, by backwards induction, create a theory to predict market action and the general qualities of equilibrium.

We posit a good j sold by seller j to buyer i . The item is listed at a price p , and has a value of V_i to the buyer. Both buyer and seller have initial, publicly known, reputations r^b and r^s . Reputation serves as a proxy for the probability that the individual will act honestly. The model incorporates a signal extraction problem: honest behavior can be perceived as dishonest. A package may fail to arrive because it was intercepted by LE (honest), or because it was never shipped (dishonest). We create a variable, r^c , representing signal clarity. r^c takes a value from 0 to 1; 1 implies perfect signal transmission, and 0 complete signal failure. There is a probability, $(1-r^c)$, that an honest signal is received as dishonest. Reputations are therefore imperfectly updated.

Production for a single unit of good j costs c , which includes production costs as well as shipping costs in most cases (many sellers offer free shipping). Finally, actors discount future periods by β_i and β_j . Each of these discount factors depends on the buyer and seller's time preferences.

The seller takes the first step, creating a listing. The seller sets all aspects of this listing: product, price, and method of payment. Product description and price have an unbounded set of possibilities, and equilibrium occurs within the intersection of this possibility set and the buyer's demand set. Assume that buyer and seller interact within this intersection. Action outside of this intersection is uninteresting; no trade occurs.

The meaningful choice we are left with at this node is method of payment. The seller chooses what occurs first: buyer payment or seller shipment. If the seller requests that the buyer finalize early (FE), the buyer pays for the product before shipment. We analyze buyer pays first.

The buyer's decision in the case of 'buyer pays first' is simple. Do I value the item above the cost? Similar to Houser's treatment of reputation and value, any purchase must satisfy the equation

$$(1) \quad p \leq r^s V_i$$

The expected benefit to the buyer must be greater than the price of the item. If this equation holds, the buyer will make the purchase. Otherwise, no transaction occurs. We assume, in equilibrium, that the seller will raise price until the previous equation is binding, that is

$$(2) \quad p = r^s V_i$$

The seller now faces the decision to be honest or cheat. If the seller is honest, item j is shipped and the seller's reputation increases. If the seller cheats, item j is not shipped and the seller's reputation decreases. Because price is a function of seller reputation, honest sellers can charge premiums. The price that an honest seller can charge is p_h and the price that a cheating seller can charge is p_c . Cheating once followed by honesty results in a payoff of $p + \sum_{t=1}^{\infty} \beta_j^t (p_c - c)$. The payoff to honesty is thus

$$(p - c) + r^c \sum_{t=1}^{\infty} \beta_j^t (p_h - c) + (1 - r^c) \sum_{t=1}^{\infty} \beta_j^t (p_c - c) .$$

The actions of the seller alter his reputation, such that it increases with honest action and falls with dishonest behavior. The reputation of an honest seller is thus r_h^s and the reputation for a dishonest seller is r_c^s . Put mathematically, $r_c^s < r^s < r_h^s$. Recall that in equilibrium $p = r^s V_i$.

Thus,

$$(3) \quad \sum_{t=1}^{\infty} \beta_j^t (p_c - c) < \sum_{t=1}^{\infty} \beta_j^t (p_h - c)$$

$$(4) \quad R_h = \sum_{t=1}^{\infty} \beta_j^t (p_h - c)$$

$$(5) \quad R_c = \sum_{t=1}^{\infty} \beta_j^t (p_c - c)$$

Equation (3) demonstrates that the expected future revenue stream from honesty is strictly larger than that from cheating. This is because honesty raises a seller's reputation, allowing seller j to charge premium prices indefinitely. These revenue

streams are simplified to R_h and R_c in equation (4) and equation (5) respectively. We can now analyze the conditions under which a seller will remain honest. Need to redefine r^c etc.

$$(p - c) + r^c R_h + (1 - r^c) R_c \geq p + R_c$$

$$(6) \quad r^c (R_h - R_c) \geq c$$

A seller remains honest when the expected cost of cheating is greater than or equal to the cost of production. Honesty is increasing with both signal clarity and future returns to high reputation. It is decreasing with future returns to cheating and cost.

$$(R_h - R_c) \geq \frac{c}{r^c}$$

A buyer has no way of knowing that equation (6) holds, instead inferring the seller's honesty through r^s . The buyer's decision being unaffected by equation (6) suggests that equilibrium is reached. Attention should be paid to three facets of this equilibrium. As previously mentioned, the seller will raise price to meet the buyer's valuation, $p = r^s V_i$. Increases in the return to honesty, $(R_h - R_c)$, will make the equilibrium more stable. The signal of an honest seller will be stronger if sellers are incentivized to be honest because the signal clarity is important for trade reoccurrence.

Now, the case of 'seller ships first.' The buyer still purchases when $p \leq r^s V_i$, but the seller now assumes all risk; r^s is effectively 1. If the expected product is not delivered, the buyer will withhold payment at no loss.

The seller's choice is to engage in the transaction, or decline. When the expected revenue exceeds the expected costs, the seller engages in the transaction

$$(7) \quad r^b V_j \geq r^b p \geq c$$

A seller remains in the market while equation (7) holds. Unlike r^s , r^b is not known.

Buyers do not have public reputations, thus r^b is the average expected buyer reputation.

After receipt of good j , buyers choose to cheat or be honest. Cheating buyers withhold payment, and receive a payoff

$$(8) \quad V_i + (1 - r^c) \sum_{t=1}^{\infty} \beta_t^c (V_i - p)$$

honest buyers receive payoff

$$(9) \quad (V_i - p) + \sum_{t=1}^{\infty} \beta_t^c (V_i - p)$$

When the seller doesn't receive payment, either the buyer is cheating or the good was intercepted. If seller j believes the buyer is honest, trade may occur again. Combining both equations gives conditions of buyer honesty.

$$(10) \quad r^c \sum_{t=1}^{\infty} \beta_t^c (V_i - p) \geq p$$

This inequality states that when the future benefits from trade, discounted by signal clarity, exceed price the buyer will behave honestly. It is important to note that lowering price unambiguously makes equation (10) more likely to hold. This incentivizes the seller to lower price until equation (7) binds

$$(11) \quad r^b p = c$$

A few qualities of this equilibrium emerge. Honest buyers enjoy a surplus of $V_i - p$, because a surplus of 0 would cause equation (10) to not hold. This surplus allows the

market to function, by rewarding honest buyers at the expense of cheaters. Price is a function of production costs as well as buyer reputation. Market durability is increasing in r^c and β_i . V_i can have positive effects, but it depends upon the marginal cost increase of an increase in value.

The addition of more buyers and sellers strengthens the market. The equalities previously derived now apply to the marginal buyer and seller. Different V_i 's, β_i 's, and β_j 's may allow some to benefit more than others in equilibrium. In the case of buyer 1st, equation (2) will still hold. The increase in market size will likely drive equation (6) to the binding point. Seller entry will put downward pressure on the returns to reputation, until entry ceases at the binding point.

$$(12) \quad r^c(R_h - R_c) = c$$

Plugging equations (4) and (5) into (12) generates an enlightening equation for seller patience

$$r^c \left[\sum_{t=1}^{\infty} \beta_j^t (p_h - c) - \sum_{t=1}^{\infty} \beta_j^t (p_c - c) \right] = c$$

$$\frac{r^c \beta_j}{1 - \beta_j} (p_h - p_c) = c$$

$$(13) \quad \frac{\beta_j}{1 - \beta_j} = \frac{1}{r^c} \frac{c}{p_h - p_c}$$

The marginal seller in equilibrium must discount the future such that (13) holds.

Similar price pressure will occur in the case of seller 1st. The price equation, (11), still holds. Taking equation (10) further calculates an equality similar to (13)

$$(14) \quad \frac{\beta_i}{1-\beta_i} = \frac{p}{V_i - p} \frac{1}{r^c r^e}$$

The marginal buyer has a β or V_i low enough to make equation (10) binding.

5. Empirical Method

Recall that in ‘buyer pays first’ equilibrium, the price of j is given by equation (2).

Thus, by taking logs of both side

$$(15) \quad \ln(p) = \ln(r^s) + \ln(V_i)$$

The log of price is a function of the observable seller characteristics, r^s , and the observable item value, V_i . Because our data contains sellers of multiple products, we expect heteroskedastic errors correlated by seller. This equation can thus be estimated using generalized least squares and standard regularity conditions. We follow the basic estimation method used in Houser and Wooders (2006).

In addition, equation (13) can be estimated. We don’t have sufficient data to attempt equation (14), because buyer’s personal values can’t be directly observed. To empirically estimate equation (13), we first make a slight transformation.

$$(16) \quad \frac{\beta_j}{1-\beta_j} = \frac{1}{r^c} \frac{c/p}{[(p_h/p) - (p_c/p)]}$$

Our previous regression will estimate for us $\frac{p_h}{p}$, the percent increase in price given one more positive review. Assuming linearity in returns to reputation, the percent decrease in price given a negative review will equal the increase given a positive review. Thus,

$$(17) \quad \frac{\beta_j}{1-\beta_j} = \frac{1}{r^c} \frac{c/p}{(2 * p_h/p)}$$

In a market with mixed payment methods, such as our data set, we assume that price fulfills a combination of equation (1) and equation (7), price is less than or equal to $r^s V_i$ and greater than or equal to c/r^b . This means our estimates will be imperfect, but can be checked later for robustness. In theory, competition will minimize this gap. Therefore,

$$(18) \quad \frac{\beta_j}{1-\beta_j} \approx \frac{1}{r^c} \frac{r^b}{(2 * p_h / p)}$$

We later estimate r^b and r^c .

6. Data from the Silk Road

We use sales data on 119 cannabis listings from 41 sellers, for a total of 9,604 sales. Transaction volume ranges from a single sale to 688. Though they can be used in a variety of ways, cannabis products have a single purpose. We assume that different strains are highly competitive, and similarly that if a well-recognized strain exists it doesn't command a premium. Our data set is parsed from the Silk Road website and covers an 11-month time period, from the opening of Silk Road II in November 2013 to our collection date in October 2014. We chose cannabis sales exclusively because it is one of the biggest portions of the market with a lot of differentiation of product type and strain. We also want to look into one type of market, presuming the marketplaces for other products are differentiated.

It is important for our empirics that we use data on sales of marijuana for personal use. Our theoretical model requires that item value assessments must use private values, not common values. In Virginia, the cutoff for misdemeanor possession charges is less than ½ oz, or approximately 14 grams. Anything above ½ oz is considered intent to sell,

and carries a felony charge. By contrast, Florida draws the line at 20 grams. Our data has a fairly natural break at 15 grams, so we will perform empirics on weights of 15 grams and below, ensuring that we ignore listings meant for resale.

6.1 Data Collection Procedure

Data was collected from the Silk Road (silkroad6ownowfk.onion) using a web crawler called HTTrack. HTTrack utilized the Tor network to download the web pages and structure of the Silk Road over the course of four days in early October. This was a slow process; the Tor network limited the download to around 4 KB/sec. To economize on bandwidth, the download ignored all images and only downloaded the text of web pages. The Appendix includes sample web page images in Figure 3 and Figure 4. The downloaded webpage data was then used to create a local mirror of the site.

Data was then parsed from the site into an Excel file using a custom parser. This created three unique data sets: seller data, feedback data, and item data. Our focus for this paper is the item data. Our parser gathered data on the listing name, price, aggregate item feedback values, aggregate seller feedback values, free shipping, number of sales, days sold for, and weight.

We will now outline some of the major difficulties with the data. The crawler is imperfect, and known to make mistakes. Of the over 30,000 files downloaded, HTTrack reported approximately 300 errors. Given the extended download period, nature of the connection and size of the download, these errors were expected. The key is that they are random. Errors typically occurred singly, at a rate of a few an hour. Also, few errors completely eliminated information on a seller or listing. Rather, they removed a page of

feedback details for a user. Finally, errors didn't change any data points; it instead makes them unreadable.

Price data also presented complications. Bitcoin (BTC) prices can fluctuate dramatically. To alleviate this, the Silk Road appears to pin listing prices to some more stable currency. The mechanism is not public knowledge, but we theorize that seller's indicate a price in USD that is then converted to BTC. This value is then periodically updated as the conversion rate changes. This creates problems when downloading over multiple days, as relative prices change due to adjustments in BTC exchange rates rather than value. To correct for this, the parser converted BTC prices to USD based upon the date of download and exchange data from the Coindesk.

Weight is our restrictive variable. The Silk Road provides no universal way to list the products weight, which creates complications for the parser. Some listings show weight in the title, others somewhere in the description. Different countries deal with decimals differently; one may list 3.14 grams, another 3,14 grams. Finally, 'grams' can be abbreviated as g, gr, or omitted entirely in the case of 'sample packs'. The parser was created to grab as many weights as possible, but could not grab them all. For future work, we will likely enter more data by hand.

The key difference in our model between 'buyer pays first' and 'seller pays first' is the price function. In 'buyer pays first' price is determined by the reputation of the seller and the value of the good. In 'seller pays first' it is a function of production cost and the reciprocal of buyer reputation. The Silk Road is a mixture of both systems.

Silk Road uses two payment methods: finalize early and an escrow system. FE closely approximates our Buyer 1st model previously outlined. A seller requires that a buyer complete payment before the item ships. Escrow is similar to Seller 1st, but imperfect. A buyer indicates willingness to purchase by sending funds to the Silk Road's escrow account. When the item arrives the buyer is then expected to release the funds to the seller. If the item doesn't arrive, the Silk Road fully or partially refunds the buyer. Typically, this favors the buyer, who receives a full refund. In terms of our model, this system works to increase r^b and r^e by raising the cost of cheating.

It is difficult to determine what payment method a seller offers. Many shift over time, depending on the item, or perhaps offer both (with bonuses to FE). Our data covers a unique period in the Silk Road's history; the centralized escrow account was hacked on February 13th of 2014. This pushed sales to mandatory FE for approximately 2 months before allowing individual choice again.

6.2 Variables Used in Empirical Analysis

Our dependent variable, *lnPricebyWgt*, is the log of an item's list price divided by its weight in grams. As previously mentioned, the price is converted to USD from BTC using Coindesk price data. Weight is converted from its list unit to grams. This creates a value in USD/gram. Listings with no feedback, either because no sales have been made or feedback posted (we cannot differentiate between the two), are ignored.

Our seller reputation variables are *VendorRatingOverall*, *VendorRepFall*, *ItemRatingOverall* and *ItemRatingSum100*. *VendorRatingOverall* aggregates seller feedback. Sales are concluded when a buyer leaves a feedback rating, from 0 to 5 stars.

This feedback is averaged over the life of the listing and reported on an item and seller's listing page. *VendorRepFall* is a dummy variable capturing dynamic effects of reputation. Buyers observe three measures of reputation: overall, 60 day, and 30 day. *VendorRepFall* takes a value of '1' if 30-day reputation is less than overall reputation. We include *ItemRatingOverall* and *ItemRatingSum100* are 3 seller reputation variables though they appear to be value related. Firstly, Item Rating and Vendor Rating are highly correlated; Vendor Rating is an aggregate of a sellers' Item Ratings. In addition, feedbacks don't typically include value assessments. They are a bimodal distribution: 5 if the good is received, 0 if it isn't. Thus, ratings better reflect a seller's honesty than the goods quality. *ItemRatingSum100* is the sum of feedbacks for the item. This is calculated by multiplying overall feedback by number of feedbacks, then dividing by 100 to make the numbers more manageable. This coefficient will be used to estimate (18). It is worth noting that we do not include number of feedbacks in our regressions due to its strong correlation with *ItemRatingSum100*. Finally, *ItemRepFall* is a dummy variable similar to *VendorRepFall* for the item rating.

Our item value variables are *WgtGrams*, *FreeShip*, *NumFeedbacks*, and *Advert*. *WgtGrams* is a variable, measured in grams, which controls for the weight of the product. This controls for quantity discounts. *FreeShip* is a dummy variable, which takes a value of '1' if the seller offers free shipping. It is difficult to disentangle the various shipping options offered by seller. This variable captures the added value of free shipping. *NumFeedbacks* is the number of feedbacks received on this listing. Higher sales numbers may signal to potential buyers that the product is as advertised. *Advert* is a dummy that

takes a value of one if the following words appear in the listing name: Premium, AAA, High Grade, Top Quality, or Strong. Marijuana's varying levels of quality are difficult to measure. This dummy weakly controls for quality differences among listings. These only hold analytical strength if we assume both that buyers can tell the difference between high and low quality product, and sellers communicate quality through these words.

7. Results

Table 1 – Summary Stats

	Variable	Obs	Mean	Std. Dev.	Min	Max
Dependent Variable	PricebyWgt	119	14.88	5.56	4.06	32.04
	PriceUSD	119	58.39	51.48	4.30	360.76
Seller Reputation	VendorRatingOverall	119	4.84	0.20	4	5
Variables						
	VendorRepFall	119	0.57	0.50	0	1
	ItemRatingOverall	119	4.86	0.21	4	5
	ItemRatingSum100	119	3.94	0.49	.04	33.64
Item Value Variables	Advert	119	0.15	0.36	0	1
	FreeShip	119	0.66	0.48	0	1
	NumFeedbacks	119	80.71	108.59	1	688
	WgtGrams	119	4.70	4.47	.5	15
	ItemRepFall	119	0.40	0.49	0	1

The results of our GLS regressions estimating (15) are presented in Table 2. We report 7 regressions, exploring different measures of seller reputation and controls. The

regressions provide evidence supporting the hypothesis that reputation provides a premium.

Our estimates of *ItemRatingOverall* are significant across all the regressions it is included in. The magnitude of the coefficient overshadows our other controls. In contrast, *VendorRatingOverall* is only significant in regression (4). It is insignificant and has the opposite of expected sign in the presence of *ItemRatingOverall*, suggesting that most reputation information is contained within the item's rating rather than the vendor's rating. *ItemRatingSum100* is insignificant in all regressions, though the addition of more controls raises its Z score. It maintains the expected positive sign throughout.

VendorRepFall and *ItemRepFall* return expected results. Given the item value controls, they are significant and negative. Despite the insignificance of *VendorRatingOverall*, changes in the rating are related to changes in the price. Changes in seller rating may be more important than the actual rating because of the inherent risks of these transactions. Sellers face forces largely outside of their control (law enforcement) and can expect a percentage of shipments to be intercepted. A stable, less than perfect, seller rating reflects this. When buyers observe a fall in a vendor's rating, there is thus confusion about the source: seller behavior or law enforcement action.

Estimates of *WgtGrams* are as expected, negative and significant. This indicates a bulk discount of sorts; the more grams purchased the lower the price per gram. *Advert* and *FreeShip* are both significant and negative. We theorize that this is because lower quality (and thus price) goods compete on more margins than high quality specialized

goods. Free shipping and quality descriptions are thus more likely for a low quality good to entice buyers from competitors' products.

Table 2 – GLS Regressions of Effect of Reputation on Log Price per Gram

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Variable							
<i>VendorRatingOverall</i>	-0.098 (0.50)	-0.109 (0.55)	-0.130 (0.64)	0.477 **(4.62)			
<i>ItemRatingOverall</i>	0.693 **(4.14)	0.694 **(4.09)	0.728 **(4.2)		0.547 **(8.06)		0.546 **(8.30)
<i>ItemRatingSum100</i>		.0027 (0.63)	.0037 (0.73)			.0056 (1.48)	.0049 (1.68)
<i>VendorRepFall</i>			-0.000 (0.00)	-0.079 *(2.33)	-0.062 *(2.31)	-0.087 **(2.61)	-0.066 *(2.44)
<i>ItemRepFall</i>			-0.032 (0.61)	-0.080 **(3.08)	-0.067 **(3.18)	-0.088 **(3.38)	-0.082 **(3.61)
<i>FreeShip</i>				-0.145 **(4.45)	-0.131 **(4.47)	-0.110 **(2.86)	-0.130 **(4.53)
<i>WgtGrams</i>				-0.044 **(14.48)	-0.044 **(15.76)	-0.044 **(14.64)	-0.042 **(15.24)
<i>Advert</i>				-0.193 **(5.86)	-0.150 **(3.52)	-0.214 **(6.61)	-0.148 **(3.59)
Constant	-0.264 (0.74)	-0.225 (0.61)	-0.278 (0.65)	0.733 (1.41)	0.357 (1.05)	3.015 **(60.54)	0.343 (1.03)
Observations	119	119	119	119	119	119	119
Number of VENDOR	41	41	41	41	41	41	41

Absolute value of z statistics in parentheses

* Significant at 5%; ** significant at 1%

7.1 Estimating Beta

Now we use the estimated coefficient of *ItemRatingSum100* to estimate β_j . The coefficients are not significant, but they are consistently positive across regressions, which is what we predicted, and approximately the same magnitudes. We will show that the actual estimate matters little at this point.

$$(19) \quad \frac{\beta_j}{1 - \beta_j} \approx \frac{1}{r^c} \frac{r^b}{(2 * p_h / p)}$$

We begin using the *ItemRatingSum100* coefficient of 0.0049; regression (7) estimated the highest Z score for the variable. We first divide by 100, to determine the estimated return to a single star review. A positive review is typically 5-stars, so we then multiply this number by 5 to determine the estimated percent increase in price given a five-star review. This gives us $p_h / p = 0.000245$.

Do these results suggest that we should we expect the quality of buyers to significantly differ from that of sellers? Perhaps sellers have stronger incentives to be honest; they must make a larger investment in reputation. But because we cannot directly measure r^b given our current data set we must make some assumptions. We thus calculate β_j assuming that r^b is the average *ItemRatingOverall* (.972), the average *VendorRatingOverall* (.968), and some lesser values. Though we can't explicitly say that these ratings approximate buyer reputation, we can weakly say that they are an upper bound.

Similarly, we do not currently have good estimates of r^c . We expect signal clarity to vary greatly depending on location, package size, even the time of year. We thus see how various values of r^c affect β . An interception rate of 1% gives a value of .99, 5% gives a value of .95, etc. For example, a 5% interception rate means that for every hundred illegal packages moving passing through the postal service, 5 are confiscated. Further work needs to be done to estimate the variable.

Table 3 - β , given a $\frac{p_h}{p}$ of 0.00245

$r^c \backslash r^b$.972	.968	.9	.75	.5
.99	0.9995	0.9995	0.9995	0.9994	0.9990
.95	0.9995	0.9995	0.9995	0.9994	0.9991
.9	0.9995	0.9995	0.9995	0.9994	0.9991
.75	0.9996	0.9996	0.9996	0.9995	0.9993
.5	0.9997	0.9997	0.9997	0.9997	0.9995

As Table 3 shows, the low return to honesty appears to overshadow any considerations of r^c and r^b . This incredibly high β is intuitive given the frequency of transactions. Given this is the time preference between sales, which occur relatively frequently, we should expect the seller to not discount very much. A retailer doesn't discount sales that will occur in the evening relative to sales in the morning. Sales are typically thought of in terms of days or weeks, not individually. As a thought exercise, the average seller has been active for 10 months, and the average listing has received

approximately 80 feedbacks. This reduces to an average of 8 feedbacks per month, or two feedbacks per week, or 1 feedback every 3.5 days. Approximately 104 3.5 day sets occur every year. By taking our high (.9997) and low (.9990) estimates of β to the 104th power we can estimate an annual β range. This works out to be $0.9012 \leq \beta \leq 0.9693$, and can be converted to an interest rate so that $0.0317 \leq r \leq 0.1096$. More robust analysis of these estimates is required.

8. Conclusion

We note some possible objections to our model. This model ignores the possibility of utility of action. Utility of actions means that an individual may receive utility from the action of honest behavior. This can be added to the model by creating a constant value to one of the payoffs. A positive constant added to the payoff for honesty or payoff for cheating could simply model utility of honesty or cheating respectively. This possibility makes any estimates of β upper bounds. Our meaningful choice node is payment method. Perhaps others should be explored. Buyers and sellers may choose marketplaces on a large number of different margins, such as: market fees, network effects, intensity of competition, encryption methods, etc. These other features of markets certainly bear further research.

Our results add to the current literature on both spontaneous order and reputation systems. Like the Law Merchant, they demonstrate how a marketplace, where feedback mechanisms and reputation are the only things keeping the market functioning, can exist without government regulation. These feedback mechanisms have created an informal institutional framework within which traders exchange goods with confidence (Milgrom,

North, and Weingast, 2010). This marketplace demonstrates the shifting institutional structure of black markets in response to new technologies and threats. Silk Road cannabis sales data support the theory that investment in reputation provides a premium to sellers, creating a framework that incentivizes sellers to deliver good service to buyers, despite anonymity and an absence of ex-post recourse. Reputation's role is especially powerful in this case; it is fundamental to the community's existence.

Because sellers are able to charge premium prices due to their higher relative reputations, this incentivizes them to work to increase their reputation. This particular incentive structure further solidifies the theory that reputation mechanisms are effective. Good reputations allow sellers to make more money and sellers are incentivized to provide quality service to their customers so that they increase their reputation and thus, make higher profits. This supports the Leeson (2005) criteria for an effective signal insofar as seller reputation is readily observable, cheap for honest sellers to obtain, and costly for dishonest sellers to garner.

Our results also demonstrate that other factors are certainly at play. Our estimates of β suggest that future revenue streams may not be enough to keep smaller sellers honest. This could reveal itself as a tendency for larger sellers to dominate the marketplace, or cause other honesty-encouraging mechanisms to emerge. Markets, following the fall of Silk Road, are increasingly outsourcing escrow services. These third-party providers supply different bundles of service; it will be interesting to see which escrow features consumers cluster around.

Further research could analyze this process over a much longer period of time and track certain sellers to see when they enter and exit the market due to reputation. An analysis of the creation of transaction networks, behaviors of entering and exiting sellers, and buyer behavior are also enlightening questions to be explored.

Chapter 2: Overcoming Anonymity: How Internet Black Markets Enable Encrypted and Anonymous Exchange

1 Introduction

In October 2013, the FBI caught Ross Ulbricht, the kingpin of a massive online dark net site, The Silk Road, in a public library in San Francisco (Hume, 2013). He had broken his one main rule; he had accidentally compromised his own anonymity. The FBI was able to link his email, which was posted on a Bitcoin forum two years previously, to the creator of the Silk Road, “The Dread Pirate Roberts” (Hume, 2013). In less than three years, Ulbricht’s site had facilitated over 1.5 million transactions of illicit substances by thousands of sellers and over one hundred thousand buyers (Weiser, 2015a). In 2015, he was sentenced to life in prison, but to the chagrin of the FBI, his influence did not end then (Weiser, 2015a).

Ulbricht’s arrest acted as a sort of massively effective informal advertisement that resulted in the number of illegal drug listings across the few main internet black markets doubling in less than a year (Crawford, 2014). As one anonymous user noted “I came for the drugs. I stayed for the revolution” (Mounteney et al., 2016, pg. 79). And what a revolution it has become. Since the beginning of the Silk Road in 2011, over eighty black markets sites have surfaced, some much more successful than others, that have enabled millions more illegal transactions to take place over the internet (Black Market Risks, 2015).

During his trial in 2015, Ross Ulbricht's defense argued that this type of drug exchange is "a peaceful alternative to the often deadly violence so commonly associated with the global drug war." They contended that this type of illicit market had revolutionized this type of exchange because it provided anonymity to buyers and sellers which made it a more responsible and safe marketplace (Weiser, 2015b). Anonymity was something unique and valuable that Ulbricht's market was able to provide to (most of) its users, unlike any black market before his.

In some ways Dark Net markets are very similar to traditional on-the-ground black markets. First, they cannot rely on formal legal institutions for the enforcement of their exchange agreements because of the nature of the goods they are selling. Second, they work to keep their identity and activities free from law enforcement knowledge. However, the Dark Net markets have many features that make exchange in this medium even more complex.

Users' true identity, physical location and personal characteristics, are anonymous, even to other users (30,000 anonymous services, 2015). This results in the inability of buyers and sellers to take physical recourse ex-post if a transaction goes awry. Unlike traditional black markets, users' reputation in the Dark Net is only associated with a username, one can straightforwardly, but not costlessly, abandon a bad reputation by creating another alias. Reputation can provide a record of the successes or failures of past transactions between buyers and sellers, but what incentivizes buyers and sellers to engage in exchange for the first time? This puzzle is particularly challenging in a space where sellers are anonymous and cannot signal their commitment to the marketplace by

an investment in physical infrastructure or any infrastructure that is backed by a third party enforcer. In response to these challenges, platform providers (marketplace administrators) impose standards on buyer and sellers which create residual claimancy over the creation of information. They provide services on their platforms that align the incentives of the buyers and sellers, which allows initial interaction to take place. This allows users to overcome the problems anonymity poses to exchange.

This paper explains how the structural components of the Dark Net, namely how platform providers, sellers, and buyers interact, enable users to overcome the challenges of anonymity in the exchange of illicit goods and services. Platform providers do this by providing private governance to buyers and sellers. The way the platform providers structure their black market sites is the efficient response to the complications posed by anonymity, lack of third party enforcement, and lack of residual claimancy over information and reputation. I model the relationship between these three main groups of users, platform providers, sellers, and buyers, to demonstrate how they allow exchange to take place. These sites make up the multibillion dollar industry that is illicit exchange over the Dark Net (Taylor, 2016). They have allowed platform providers themselves and sellers to reap immense economic profit while creating a safer environment for their buyers (Weiser, 2015b). This paper primarily focuses on some of the most popular sites; Hansa, Agora, Dream Market, Silk Road 2, Valhalla, and Alpha Bay. These sites provide a wide array of platform provision, a substantial shelf life, and/or data which is used for empirical analysis.

Due to the nature of the goods and services sold on the Dark Net, empirical data is difficult to come by. Most Dark Nets sites do not provide aggregate data about their services and many law enforcement agencies are not forthcoming with their findings either. Most of the data used for this analysis was collected by parsing data from these Dark Net sites and from forums about these marketplaces and testimonies of users. I use this evidence to argue that the survival and persistence of these marketplaces is due to the incentives that the platform providers create by the services they provide.

In what follows, I examine the systemic effects of various platform structures on the Internet black market's existence and persistence and the incentives facing both buyers and sellers in these marketplaces. An overview of the Dark Net is covered in Section 2. Section 3, covers the economics of anonymity and private governance and its pertinence to the Internet black market. In Section 4, I model the Internet black market and the three main groups involved, platform providers, sellers, and buyers. I show how platform providers structure their sites in a way that fosters an environment of accountability due to the alignment of the incentives of both sellers and buyers. Section 5 provides evidence, both qualitative and quantitative, of what my model predicts. Section 6 concludes.

2 The Dark Net

Internet black market exchange is able to take place because of the conjunction of Tor and Bitcoin, which together make up the Dark Net. In order to understand the Dark Net (also known as the Dark Web), it is important to first define the Surface Web and the Deep Web. The Surface Web is comprised of content on the internet that can be found

using a search engine. If Google, Bing, or Yahoo can find certain information, it exists on the Surface Web. Surface Web information is accessible and indexed.

The Deep Web consists of information that is un-searchable by a search engine. For example, if you buy something online on Amazon, someone cannot search for your credit card information via Google. Amazon utilizes this private information and does not make it available for public use. Organizations such as public libraries and local governments and businesses such as online retailers manage a great deal of data in the Deep Web (Christin, 2012). Information on the Deep Web is estimated to be hundreds, if not thousands of times larger than information on the Surface Web (*Deep Web: A Primer*, 2012). This information is accessible but non-indexed. The Dark Net is a small subset of the Deep Web, it contains information that is restricted and non-indexed. Activity on the Dark Net that has to do with exchange is done using the Tor network (Gaup, 2008).

Unbeknownst to most, the Dark Net was not born from the technologies of drug lords, it exists because of a routing system that was developed by the United States government. In 2002 the U.S. Naval Research Laboratory developed the first generation of Tor and in 2004 they developed the second generation to anonymously communicate over the internet (Dingledine et. al., 2004). In The Tor (The Onion Router) network enables anonymous communication and transactions. The information sent via Tor is encrypted. It then travels through numerous nodes in the network. When information travels through the Tor network, messages are ‘bounced’ between nodes which makes them virtually untraceable (Dingledine et. al., 2004).

Onion routing is similar to mix-networks because messages are wrapped in layers of encryption. This encrypted information contains keys of all the intermediate nodes that the information will reach before it reaches its final destination. When the information reaches each node a layer of encryption is lost and the information continues traveling randomly throughout the network, losing layers of encryption as it goes (Gaup, 2008). This network allows for anonymous and untraceable communication because there is no correspondence between incoming and outgoing messages from each node the information travels through (Gaup, 2008). This is the most prominent form of anonymous communication, the robustness of its security lies in the diffusion of trust all through the system (Johnson et. al., 2011).

Because Bitcoin is the most popular and widely adopted anonymous crypto currency, it is used as a medium of exchange on Tor. A Bitcoin is technically a solution to a mathematical equation with a fixed set of solutions (Grinberg, 2011). They are able to be stored in a virtual “wallet”, similar to cash, and are exchanged with low transaction fees through anonymous virtual transactions (Briere et. al, 2013). This is a peer-to-peer currency that does not require verification from a central third party (Christin, 2012). Exchanges made using Bitcoins over the Tor network are extremely difficult, if not impossible, to trace.

Problems arose for some Dark Net sites because they were using centralized infrastructure which made them more susceptible to hacking and take down by law enforcement. Therefore, marketplaces began to provide software options that use blockchain technology. This type of distributed ledger technology is decentralized and

enables money to be sent directly from buyer to seller. The bitcoin blockchain is the largest of the distributed ledgers (Tapscott and Tapscott, 2016).

3 The Economics of Anonymity, Private Governance, and Club Goods

3.1 Anonymity

Anonymity is keeping one's personally identifiable information (PII), any information that could be linked back to your identity, this could be anything from your zip code to favorite restaurant, secret while communicating (Chaum, 1981). In the literature, anonymity, as a measure, is described as an element of security and vulnerability within communications. The more protected one's anonymity, the more secure one's communication is. The less anonymity one has, the more vulnerable one is to interceptions or misinterpretations of his or her communications. It is a negative state in which the user is measured by *not* being identified. Chaum (1998) describes the best case scenario is one in which full anonymity is provided to the participant and it is completely unknown if the participant was involved in any type of communication. It is characterized as a mechanism to prevent the attack of communication and to ensure privacy (Kesdogan et. al., 1998).

Any enterprise, business, or independent sellers that deals with private client data, anything from their zip-code to credit card information risks losing market share if they do not implement proper privacy practices. Sellers try to differentiate themselves by implementing rigorous privacy statements and back them up with the appropriate technological means (Dingledine and Syverson, 2002, pp. 69-84). Sellers often want to provide more personalized services on the web to fully describe the good and/or service

they are providing and to further differentiate themselves from other sellers. However, they may be resonant to disclose information so as to not reveal their true identity. If the seller reveals too much information about themselves, the information could become a proxy for the seller and could eventually lead to their exposure (Dingledine and Syverson, 2002, pp. 85-98).

It is difficult to brand one's business when anonymous. The goal of personal branding is to create a highly marketable image set apart from the competition. This might appear to be an invitation to pad one's résumé, especially since the Web is often viewed as a potential site of anonymity. Yet personal branding literature relies upon the language of authenticity, arguing the responsible self-brander is a person who is honest with herself and others. "... Branding is not about tricking people into buying your services or pretending to be someone you are not. It's about clearly establishing who you are, what you are good at, or even what you like to do, so you can stand above the competition." (Gehl, 2011).

There have been various identified solutions to overcome these challenges anonymity poses to exchange. Traditional ways to overcome anonymity include third party enforcement (Alqahtani, 2014) and the interaction of small homogeneous groups (Sassenberg, 2002; Wilson et al. 2010; Barreto, 2002, Greif, 1993). However, with the advent of exchange over the Internet, some of these traditional means are not possible to employ. Baran (1964) poses that, to overcome these problems, participants must depend on a common authority to protect their identity. Through the use of digital pseudonyms, public codes used to verify signatures made by the anonymous holder of the

corresponding private codes, any one intermediary can provide security to messages passing through it. An authority creates a roster which lists all the pseudonyms but cannot connect the pseudonyms to their user's identity. The authority also has the ability to set parameters for acceptable and unacceptable pseudonyms. This ensures that messages can be anonymously sent or received (Chaum, 1981). With a central register, it is possible for users to make a new pseudonym and maintain their reputation (Dingledine, 2003).

Although enterprises promise to keep their customer's identity and information safe, how do they overcome the problems that arise when the central system of an enterprise is compromised? In their paper, Karjoth et. al. (2002) describe a decentralized system that restricts various users from access to personal data. The system separates the duties and access of multiple "administrators" that make up a privacy system. Therefore, each party in the security system does not have complete control or access to the private information of users (Dingledine and Syverson, 2002, pp. 69-84).

Dornbach and Nemeth (2003), discuss the tradeoff that sellers face between privacy and personalization. They show how sellers can personalize their goods and services without compromising their anonymity. They suggest separating identity and profile in a way that reveals information about the product and service without exposing the seller's personal information (Dingledine and Syverson, 2002, pp. 85-98). Private credential technologies can "allow the user to prove things about himself without revealing extra personal information (Dingledine and Syverson, 2002, pp. 18). Most prominent of these technologies is digital certificates, which enable buyers and sellers to

use the security infrastructure, Public Key Infrastructure (PKI), that provides for internet and e-commerce communication (Brands, 2000). Digital certificates enable a user to exchange information safely and securely over the internet, like an electronic passport (Rouse, 2013).

Incentives to participate in a communication or market system that relies on anonymity can pose a substantial threat to those systems' success and survival. Acquisti et al. (2003) investigate the incentives of users to offer and use anonymity services. It is critical to align incentives "to create an economically workable system for users and infrastructure operators" (2003, pg. 84). Individual users cannot secure their own anonymity through a network system. Systems that successfully align incentives are ones that rely on a central authority that administers infrastructure which provides protection by distributing information. This authority has residual claimancy over the infrastructure and the information it generates. Each user runs a node in a shared information network, only if the benefits of doing so outweigh the costs. With this decentralization, users can be assured that their information will never be uncovered, even if there are a few colluding users (Acquisti et al., 2003)

Ioannidis et al. (2009) suggest successful organizations that are in the business of information security make tradeoffs between privacy and availability. Defenses deployed against one may compromise the other. In order to protect both, many organizations expand the distribution of their servers to maximize their attack surface. Anonymity can pose a challenge to market activity because it makes trust difficult to establish, due to high monitoring costs between traders. Spiekermann et al. (2015)

find that organizations that use personal information do so to lower transaction costs for their users and for themselves. However, they suggest that the possession of this sensitive information can be as much of a burden as an asset. To secure this information, organizations have to update their security technology and adjust their organizational processes constantly (Spiekermann et al., 2015). To prevent free riding in the network, (Acquisti et al., 2013) suggest charging a usage fee for participation in the platform. Networks are most successful if users have a vested interest in an anonymous network. Reputation mechanisms also provide incentives for users to benefit each other in order to receive public recognition.

Manshael et al. (2013) model anonymity and network security using game theory. They find that the security of a network can be viewed as a social (club) good. Participants in a particular network group benefit from the security provided by the network. The fate of those in the network is intertwined. Everyone using the network benefits from the security measures and everyone suffers if the network security is compromised.

3.2 Private Governance and Club Goods

In areas or marketplaces where formal government is scarce or non-existent, self-enforcing arrangements can act as a substitute for formal third party enforcement. The lack of a formal third party enforcer increases the likelihood of fraudulent behavior. Stringham (2015) discovers how technically advanced markets can function even when fraud is rampant. PayPal and other online intermediaries set up *ax ante* risk management mechanisms that mitigate danger in the marketplace. These intermediaries charge

transaction fees, higher fees for high-risk areas. This type of trade is still able to take place because higher risk premiums for fraudulent activity, on the margin, discourage fraudulent trade. Leeson (2005) studies the political economy of Africa, wrought with the problems of both social heterogeneity and violence. He finds that these people used signaling to enforce anarchic exchange with heterogeneous groups. This informal mechanism acted as private governance, it is self-enforcing and governs interactions.

Greif (1993), from his analysis of the Maghribi Traders' Coalition in the 11th century, finds that an informal economic institution can overcome commitment problems to exchange. These institutions were successful because they were able to enforce trade contracts as well as support "the operation of a reputation mechanism" (1993, pg. 525). Zerbe and Anderson (2001), suggest that cultural concepts, such as fairness, created norms and eventually institutions that traders will uphold. Some institutions enforce anarchic exchange through exclusion. Stringham (2002), through his study of the London Stock exchange, finds that it emerged as a self-policing club. Members of the group would exclude nonmembers and remove those who were not following the rules.

Criminal organizations mitigate risky behavior by providing private governance in the form of club goods. Among the most critical of these club goods are security services and conflict resolution services. Gambetta (1996), argues that the Sicilian Mafia was in the business of private protection. This crime group was able to guarantee the safety of both parties engaged in illegal transactions, allowing this type of exchange to persist. Skarbek (2010; 2011; 2012), finds that Prison Gangs, in California Prisons, provide protection for their members against other violent inmate groups. Piano (2017),

finds similarly, in Outlaw Motorcycle Gangs, that these criminal organizations provide club goods and private governance to their members in the form of personal security services.

4 A Model of the Internet Black Market

One solution to the problem of anonymity in an extralegal environment is for a decisive party to internalize the costs and benefits of governance by providing an infrastructure that aligns the incentives of users. They do this by providing private governance to their users to encourage and foster repeated trade. Instances of private governance provision have included; signaling, exclusion of defective users, and the provision of club goods.

4.1 The Anonymity Problem

To demonstrate the logic of this argument, imagine a scenario where a buyer (B) and a seller (A) would like to make an exchange of illicit goods over the Dark Net. Due to the nature of the goods, anonymity is essential for exchange to take place. However, law enforcement (C) can observe information about identity because both buyer and seller must expose information about themselves in order for the sale of goods and successful shipment to take place. This scenario is illustrated in Figure 7, below.

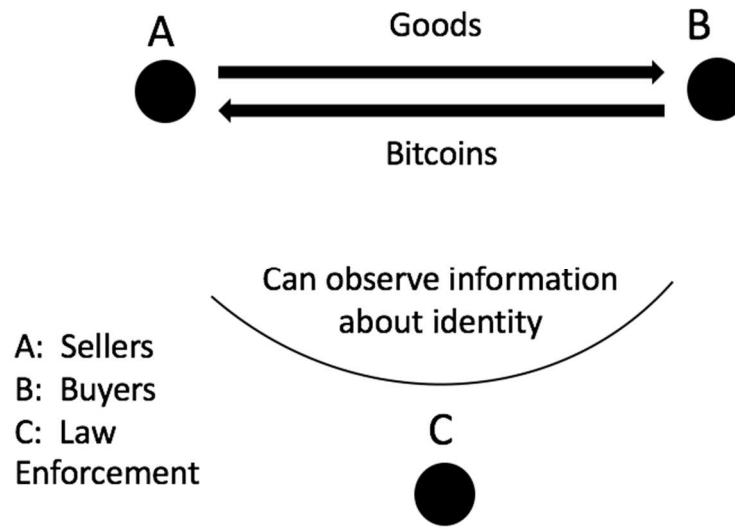


Figure 7: Initial Scenario

The exchange itself is not problematic per se, the technology is in place for this type of exchange to occur over the Internet. However, with no third party enforcement and the exchange of illicit substances, how can transactions on the Dark Net reliably and repeatedly take place? Buyers will likely buy from sellers with a good reputation, which is evidence of previous successful transactions, but what would incentivize buyers and sellers to exchange at t_1 ? Because there is no access to a formal third party, informal mechanisms and institutions can emerge to substitute for this (Leeson 2002; Greif, 1993; Stringham, 2015).

These mechanisms can act as private governance for a market that is unable to benefit from formal governance. Exchange, however, can and often does reveal the identity of the parties involved in order to facilitate repeated trade. This information

would then be available to law enforcement and would jeopardize the safety of the marketplace. Therefore, some of the mechanisms that reveal personal information about buyers and sellers that traditional private governance would provide are not an option in the Internet black market.

Entrepreneurs in the Dark Net are alert to profit opportunities posed by the challenges buyers and sellers face in this market environment. Platform providers internalize the benefits of securing privacy in this environment. They introduce institutions that protect buyer and seller anonymity, allowing exchange to take place without revealing information to law enforcement. Each platform is independent of other platforms in its platform structure, user criteria, selection of illicit goods and services to sell etc. Platforms compete with one another for users in this marketplace. Creating a platform for the exchange of illicit goods and services over the Internet black market is a relatively high cost activity. Providers need extensive know-how of the routing system, various code bases, encryption methods, and branding techniques. Given these conditions, each platform provider's revenues at the end of every period is r , assuming size is constant across platforms.

The platform providers face a tradeoff between the protection of users' privacy (anonymity) and availability of their market information, to increase their revenues. They could increase their revenues, in the short run, by limiting the resources they devote to privacy protection. However, this tactic would limit their availability capabilities in the long run because fewer users would feel safe on their platform. With a large number of

users with imperfect information about other users would drive security costs up, opening the door to fraudulent behavior, thus making exchange much more difficult.

These problems to Dark Net exchange could be solved if the platform providers acted as a governing body that aligns the incentives of their users, both buyers and sellers, illustrated in Figure 8.

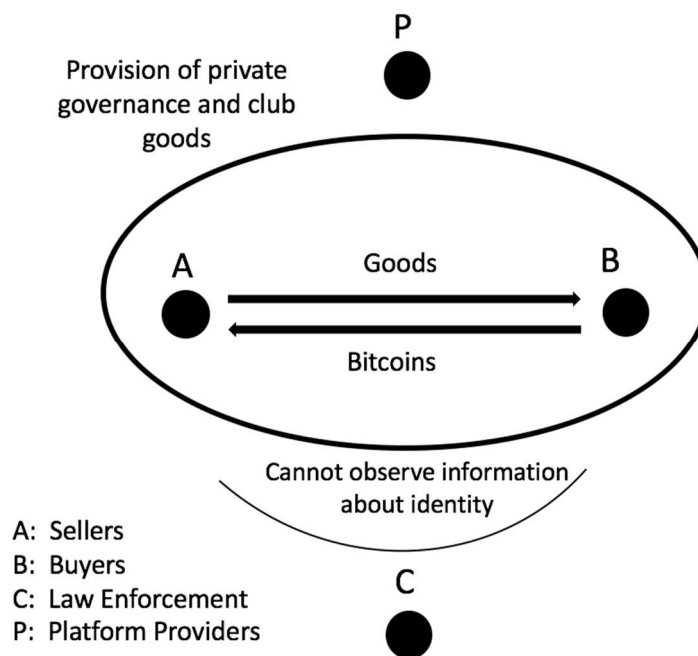


Figure 8: Provision of Private Governance and Club Goods

Platform providers achieve this by providing private governance that fosters initial and repeated trade. They become the residual claimant of the platform and the information that is generated by and passes through the platform. Platform providers allow buyers and sellers to reveal information about themselves without disclosing any personal

information. They also protect their users from vulnerability to law enforcement. Under this new platform structure, each platforms' revenues increase to β , $\beta > r$.

This increase in revenues comes from the reduction of fraud and law enforcement engagement, due to the provision of private governance. The platform providers employ tools that guarantee the robustness of the market. The adoption of private governance provision brings the benefits of increased revenue, however, each platform has to contribute, c , to finance the governance and security operations. Therefore, private governance will be provided on Dark Net platforms as long as the benefits of protecting anonymity outweigh the costs; $\beta - c > r$. Therefore, the benefits of providing private governance will depend on the amount of fraudulent user behavior and amount of law enforcement effort applied to compromise user anonymity. The techniques platform providers employ to secure institutions that protect illicit and anonymous exchange are discussed in Section 5.

5 Evidence

The structure of Internet black market sites and information about user experiences on them offer strong evidence for the validity of my analysis. The prevalence of these sites has increased exponentially since their beginning in 2011, as shown in Figure 9. The evidence also supports the theory of how exchange can exist with anonymity how and why organizations provide private governance.

5.1 Private Governance in The Dark Net

As (Zerbe and Anderson, L, 2001) suggest, creating a culture of common values is essential to making mechanisms of private governance self-enforcing. Platform

providers go to great lengths to create community on their sites. The ‘Dread Pirate Roberts’ (Ross Ulbricht) encouraged community members to be engaged and aware (Mounteney et al., 2016). Silk Road forums included topics from philosophy to movie suggestions. Cryptomarket forums provide a platform for users to perpetuate and share their culture and priorities. Drug Safety forums are some of the most popular. Users will share their knowledge of law evasion, chemistry, the dangers of drugs, and drug rehabilitation (Mounteney et al., 2016). One user notes:

The community here is awesome. There is a “Drug Safety” forum. The whole philosophy behind the place is that if you want to put heroin in your body, go ahead. But hey, if you want to get off that nasty drug, we’re here to help you too. It’s not like real life where street dealers might coerce you into keeping your addiction. (Van Hout and Bingham, 2013, pg. 527)

These illicit markets rely on trust. It is possible for a seller to send a buyer fraudulent goods or goods that could greatly harm the buyer. If users did not trust the fact that other users would not do this, the market would be unable to function (Mounteney et al., 2016). A Silk Road site administrator notes “Our community is amazing [...] [users] are generally bright, honest and fair people, very understanding, and willing to cooperate with each other” (Chen, 2011).

Anonymity the central component of the Internet black market culture, “sellers feel comfortable openly trading hardcore drugs because the real identities of those involved in Silk Road transactions are utterly obscured” (Chen, 2011). Sites provide guidelines for users, both buyer and sellers. Dream Market includes extensive buyer

guidelines that include securing user's account, bitcoin usage, PGP protection tips, and escrow protection (Introduction, 2017). Kruithof et al. (2016), analyze the rules of ten different cryptomarkets and find that the most commonly emphasized rule was to protect anonymity and reduce third-party (law enforcement) harm.

5.1.1 Residual Claimancy

Sites on the Internet black market have two levels of authority that provide governance, the platform provider, also known as the administrator, and the moderator(s). The platform provider owns the website. He or she manages the website and sets up how it is run (Mounteney et al., 2016). The platform provider can authorize accounts, make new product categories, and restrict the sale of certain goods. Providers can and do also close down fraudulent user accounts (Forums: Dream Market, 2017; Forums: Hansa, 2017). They create the details of the platform where exchange takes place. Their most important tasks are security of user anonymity and security which facilitates the marketplace (Mounteney et al., 2016). The moderator works under the platform provider. Moderators have limited access to user information and administrative power. They primarily scan forums and site pages for fraudulent deals and answer user questions (Mounteney et al., 2016, pg. 79). Figure 10 shows the Support page on AlphaBay Market where users can submit support tickets to moderators with questions about the site, their page also includes their PGP key (will be discussed shortly). Wall St. Market also uses a ticket system to answer user questions (Support: New Ticket, 2017).

Mounteney et al. point out “one reason crypto markets can operate so ‘successfully’ is that they employ strict self-regulation. Both the cryptomarket

administrators and moderators ensure that buyers and seller comply with the rules imposed on them” (Mounteney et al., 2016, pg. 79). Platform providers facilitate this type of self-enforcement by aligning the incentives of buyers and seller which not only allows for exchange at t_1 but t_n as well.

Platform providers do this by setting up reputation systems to mitigate complications with anonymity and trust. They provide their users with rating systems, reviews of products or sellers themselves, feedback platforms, and communication forums. These reputation systems allow users to view the seller’s previous transaction history. Through the reviews about the product itself and feedback about the seller, the potential buyer can make an educated assessment of whether or not they are willing to make a transaction with this individual, based on their perceived trustworthiness. These reputation mechanisms incentivize sellers to provide their buyers with quality products because they can charge a premium for their goods if they have a good reputation (Hardy and Norgaard, 2015). Cryptomarket users have indicated that review and feedback mechanisms are one of the main reasons they have choose to buy illicit substances over the Internet, it makes them feel more safe and confident with their purchase (Barratt et al., 2014)

When a sale between a buyer and seller has been verified, the platform allows the buyer to leave feedback on the seller page, this come in the form of a rating, a star rating between 0 and 5, and verbal feedback. Figure 11 and Figure 12 show a vendor page on Dream Market and AlphaBay Market respectively. Most markets use a star rating system out of 5, but as you can see, AlphaBay uses a “Vendor Level” system where the seller is

rated between 0 and 10 (Listing Options: AlphaBay Market, 2017). Feedback about previous buyer's experiences help to keep the sellers honest. They give other buyers a feel for what is good or bad about the products being sold. Figure 13 shows extensive feedback on AlphaBay Market for MDMA. Figure 14 shows just one user's feedback on a cocaine product sold on Wall St. Market.

Van Hout and Bingham (2013) conducted extensive interviews of users of the original Silk Road. Survey participants pointed to the site's vendor feedback ratings as a primary reason for using the site. One respondent, a male aged 26-30 years, noted; "the feedback system is revolutionary for a market like this. All my fears about quality are gone. I know when I'm getting and I know that it's good" (2013, pg. 526).

5.1.2 Exclusion

Users have expressed that the entry costs of the Internet black market are high, but the benefits outweigh the costs. A survey participant noted "The Silk Road is a paradise for responsible drug dealers. You have to be patient and you have to be smart to get there and use it. Bitcoin isn't easy to get and use. You have to learn the ropes. But it's totally worth it. It's changed my life significantly" (Van Hout and Bingham, 2013). To become a vendor on Hansa, for example, you have to submit an application and be approved by the administrators. Vendors can be labeled as a "trusted vendor" if they have 100 or more positive feedback reports and are in good standing with other markets they are selling goods on as well (Knowledge Base and Support, 2017).

In an attempt to exclude sellers that are likely to try an exit scam, a situation where a seller sets up shop with no intention of continuing it after the first sales, scams

the buyers, and pulls out of the market with the money, cryptomarkets charge sellers a set fee for becoming vendors on their site. To become a seller on AlphaBay, the user must pay a set \$200 fee (Fee for Becoming, 2016). This fee makes it much more difficult for a seller exit scam to be profitable and thus, deters a lot of potential scammers.

Site admins reinforce the rules of the site by applying sanctions on defective users. If they find that a user is engaged in fraudulent activity, they will withdraw their user account. (Mounteney et al., 2016, pg. 79). Figure 15 and 16 show two vendors who were banned from Hansa (Forums: Hansa, 2017). Dutchexpress (Figure 15) was a vendor who did not resolve numerous buyer disputes and was accused of scamming other buyers. Royaldrug (Figure 16) was also banned because they scammed multiple buyers (Forums: Hansa, 2017). The DarkNetMarket Reddit page also provides extensive discussion about numerous cryptomarket scams and prevention mechanisms (Vendor CandyNL, 2017).

5.1.3 Advertising

One way markets advertise their security measure is by investing in the code base they build their market on. Various code bases include Custom², Nette, Wordpress, Bitwasp, Drupal, and CakePHP (*Black Market Risks*, 2015). These various codebases

² 'Custom' here denotes that a platform provider has written their own software, typically the admin themselves writes the code. It is possible that the platform provider is using an existing framework but has simply hidden some of the more obvious signs of which code base it used. For example, Agora played with the HTTP headers to make it impossible to figure out what code base they were using. Platform provider admins are typically programmers. Code is extremely important for the site, therefore 'code is law' and, in practice, the real owner of a dark market site is whoever controls and programs the servers. Therefore, a non-programming admin faces a major principal-agent problem in trying to hire sysadmins or developers whose work they are not competent to understand and audit themselves (*Black Markets Risks*, 2015).

require a certain level of technical skills and employing a more technical (costly) codebase will increase the security of users from hacking and anonymity threats. Bitwasp has the reputation of being a less sophisticated and risky codebase to use. Among the 14/80+ Dark Net sites that have used Bitwasp as their codebase, 12 of them are no longer still functioning on the Dark Net. Among these sites are Hydra, TOM, Freedom Market, Flomarket, Doge Road, Silk Street, and Underground Market. The only 2 remaining sites using Bitwasp as their codebase are The Real Deal and Anarchia³. According to the analysis on *Black Market Risks*:

The death rate of Bitwasp marketplaces will always be higher because it lowers the barrier of entry to starting and launching your own BTC marketplace so less technical people with lesser funds to start the marketplace will use it and that demographic has a higher chance of failure. From a predictive standpoint, it doesn't much matter why Bitwasp correlates with shorter lifetimes - whether it's through greater likelihood of being hacked or self-selection by weak-willed/poor/uncommitted/incompetent operators. As long as it does, it'll improve predictions by predicting shorter lifetimes for Bitwasp-using marketplaces, and so it's less safe for buyers: even if the marketplace is using multisig, there's still some limited scope for an exit scam; it wastes one's investment in learning how to use a marketplace; and sellers lose any bond they put up. (2015)⁴

³ There is reason to believe that Anarchia has been recently shut down and that The Real Deal closed then was recently reopened.

⁴ There do exist vendor bonds and deposits/floats which are ways that new dark market sites can recap supra-commission rewards in a potential exit scam

The codebase of each of these active sites is available on the *Black Market Risks* (2015) website so it is readily available to potential users to view. Site builders/administrators who spend more time and money creating a Dark Net site based on a reliable codebase have a lower likelihood of being hacked and users in these marketplaces know this⁵.

To further advertise their trustworthiness, Dark Net sites partner with reliable sellers, as shown in Figure 17 and Figure 18. This can be costly because Sites are taking a risk by vouching for particular sellers. If the seller's reputation begins to decline, it will be associated with a less trustworthy site. The site also does not want to discourage other sellers from offering their products on their site because they are only favoring particular vendors. It is crucial that these sites pick and promote only their best sellers, to encourage reliable traffic on their site (Martin, 2014).

5.1.3.1 Branding

Each seller can utilize a variety advertising mechanisms, some more costly than others. Sites use nicknames, branding, advertising, mission statements, and drug purity tests. The choice of name of the seller and of the particular product communicates insider information to people who are very familiar to that market. For example, in the cannabis market, there are very particular strains of cannabis and if you would like to tap into that inner group information, using a name similar to one of a prominent strand could help achieve familiarity bias in a potential buyer. Popular names include names that are

⁵ Although many platform providers who utilized Bitwasp no longer have running sites, it doesn't directly imply that Bitwasp is an inferior code base and more research needs to be done on whether or not this is the case. Many sites function for about 5 months and many, if not most, of them are inoperable within 3-4 years. Many platform providers turned to Bitwasp as a code base after Silk Road 1 got shut down so there are many confounding factors with regards to Bitwasp platform provision (Black Market Risks, 2015)

related to drug-themed TV shows like *Breaking Bad* (Martin, 2014). Other, more serious sounding names convey a higher level of professionalism and/or lack of knowledge of drug culture. Sellers use pictures and logos to construct a certain vendor identity to build their reputation, some logos are very professional looking and others look very homemade (Martin, 2014). Various types of logos convey certain associations to users, Amazon Dark, for example, is utilizing a connection most users will have with the online marketplace Amazon.com.

Mission statements are also included in many seller pages, some of these include ethical branding such as “conflict free”, “fair trade”, and “organic” products, as shown in Figure 19 and Figure 20. This suggests that some buyers are highly discerning when buying some illegal products. The validity of a mission statement is difficult to verify, however, some sites do not claim that they have the best products and will specifically advertise that their product is inferior but at a lower price. They may be doing this to preemptively manage expectations of buyers in order to avoid negative reviews. The best way for a seller’s validity to be verified is through their rating score, buyers can leave comments and quantitative review scores for each seller they purchase products from. Figure 5 shows an example of buyer reviews of a particular type of cannabis on the Silk Road 2 (Hardy and Norgaard, 2015). These reviews are a very transparent and immediate way for buyers to give immediate feedback to the sellers and to inform other buyers in the marketplace of the quality of a particular seller’s goods.

Other, costlier advertising techniques sellers use are offering free shipping, free samples, bulk discounts, more secure packaging, refunds, holiday pricing, and free

giveaways, shown in Figure 21 April 20th is the Dark Net equivalent of “Black Friday”, during this day, most sellers offer deals on products, drugs in particular, to buyers (Martin, 2014). Some sellers will offer periodic lotteries that give away cryptocurrencies or free illicit drugs to winners. Similar to a frequent shopper card that one can obtain at a typical grocery store, various vendors will offer reward programs for repeat customers that include discounts for loyalty (Martin, 2014). Figure 6 shows shipping options on a particular cannabis product on the Silk Road 2 (Hardy and Norgaard, 2015) that includes free shipping.

Due to the fact that any package that is shipping illegal products could be seized en route, the signal clarity of the seller’s trustworthiness is very noisy. If a buyer purchases a product and it does not arrive at their shipping address, the buyer does not know if the seller was dishonest and never sent the package in the first place, or the seller was honest and shipped the package but it was intercepted by authorities (Hardy and Norgaard, 2015). This makes seller commitment to refunds even more valuable. If a seller offers to send the product again or offers to give the buyer a refund if their purchase was never received, the seller is willing to incur this cost to build their reputation, regardless of whether or not it was their fault that the buyer never received their package.

5.1.4 Contract Enforcement

Platform providers enforce contracts between buyer and sellers. If a user has been wronged by another user, it is much easier for a seller to “wrong” a buyer, the platform provider will act as a third party mediator and resolve the matter. Figure 22 and Figure

23 show sellers' interactions with Dream Market site administrators and how the administrators resolved the disputes. Figure 22 shows a complaint from buyer WeedyDE2, complaining that they were scammed by their seller. SpeedStepper, an administrator says that they have unlisted and disabled further vending from that seller and notes that the seller is unable to make any more exchanges until the issues are resolved (Forums: Dream Market). Figure 23 shows a conversation between heinrich123, a buyer, and SmallWood, a moderator. The buyer did not receive his goods from seller "kushtime," so the moderator informs the buyer that the seller was banned and that (if the buyer did not finalize early) he will receive a refund from escrow (Forum: Dream Market, 2017).

5.1.5 Fraud Prevention

Like in any market, it is possible for users to commit fraud. Platform providers try to prevent this as much as possible by structuring their platforms so as to reward honest users and punish fraudulent users. Seven out of the ten sites specifically listed rules related to transaction protocol and security measures. For example, many of the sites analyzed (Kruithof, 2016) did not allow sellers to request or require their sellers to 'finalize early.' This means that the buyer has paid the seller before the buyer has verified that he or she has received the goods. This method of payment does not use an Escrow account and puts much more risk on the buyer.

The majority of Silk Road users who were survey respondents reported that the use of 'Escrow' protected them against scamming (Van Hout and Bingham, 2013). Male respondent, aged 20-25, describes his experience with Escrow; "we also use an Escrow

system so that vendor's can't scam you. So the Bitcoins aren't directly delivered to them until I finalize my order, which I only do once the package arrives. Some vendors require early finalization, but I try not to deal with them" (2013, pg. 526). Some vendors allow buyers to make their own decision as to whether or not to use Escrow services. Figure 24 shows various goods sold on Dream Market, two of them allow Escrow services, the other two do not.

Although it is more common for sellers to commit fraud against buyers, it is possible for buyers to leave fraudulent feedback on a seller's page. Hansa has specific criteria for under what circumstances it is acceptable for a seller to have buyer feedback removed, these reasons include; at the customer's request, feedback includes blackmail, feedback includes private seller information, or feedback containing extreme profanity (Knowledge Base and Support, 2017). Figure 25 details the procedure on Hansa. Users are quite confident, however, of site's abilities to prevent fraud. A survey participant noted:

I only use Silk Road. This type of market significantly lowers the chances of a scam or buying contaminated products. Like Amazon or eBay, I have a market of sellers to choose from and product reviews to satisfy my own requirements before I make a purchase. A street market in comparison is based on a "take it or leave it" approach which gives no rights to a buyer. This form of regulation ensures safety and harm reduction for the buyer.

(Van Hout and Bingham, 2013, pg. 526)

This is also evidenced by the fact that these sites still exist and continue to persist.

5.2 Provision of Club Goods in the Dark Net

5.2.1 Personal Security Services

During Ross Ulbricht's trial, his defense team did something unprecedented in a criminal defense case. They argued that Ross Ulbricht's site, the Silk Road, actually made drug use safer (Greenberg, 2015). From an ethical standpoint, they argued that Ulbricht's new method of illicit material e-commerce reduced the risks of drug use. This cryptomarket, they pointed out, protected user's anonymity, sparing them any physical interactions with traditional drug dealers (Greenberg, 2015). Cryptomarkets have made the sale of drugs safer and much less violent. Numerous Silk Road users cited safety as a reason they sought out the Internet black market rather than a traditional black market (Van Hout and Bingham, 2013). A male user, between the ages of twenty and twenty-five, testified to the safety of Silk Road; "I advocate for harm reduction and the freedom of information for individuals to use substances safely. Websites provide essential information which allows me to make rational decisions about using illegal substances safely' (2013, pg. 526).

Bitcoins are the most commonly used currency on the Internet black market. Bitcoins, however, are not a completely anonymous cryptocurrency (Chen, 2011). Bitcoins function using block chain technology. Block chain is a public ledger that includes records of all successful transactions made with the currency (Mounteney et al., 2016). Most avenues to buy Bitcoins require you to link your personal information to the Bitcoins themselves. A valid ID is often required when purchasing Bitcoins. Once the Bitcoins have been linked to one's personal identity, the transactions made with those

Bitcoins are able to be traced back to the owner. However, it is possible to buy Bitcoins anonymously, a practice widely used in the Internet black market. This ensures that the personal identity of the Bitcoin owner is not linked to the purchases the Bitcoins are used to make (Mounteney et al., 2016, pg. 42). However, there have been instances where law enforcement, through block chain analysis and sophisticated network analysis, has been able to trace some user's personal identity by linking the Bitcoin transaction back to them, although extremely difficult and unlikely (Mounteney et al. 2016; Chen 2011).

In addition to Tor, platform providers use a variety of encryption techniques to protect the privacy of their users as well as their own privacy. Some of these techniques encrypt communications, private messages, and currency exchange. A commonly employed encryption programme is called PGP. This program is set up by the platform providers for their use as well as for the use of their buyers and sellers. PGP stands for 'Pretty Good Privacy.' It is a computer program that enables encrypted messages to be sent and only the intended recipient has the ability to decrypt the message. The program also has a way for recipients to "sign" messages, as a way to further verify the recipients authenticity (Mounteney et al., 2016). This technology was developed by Phil Zimmerman as a way to protect privacy, he intended it to have multiple uses, for anything from messages about relationships to message about political dissent (Zimmermann, 1999).

PGP users have two pairs of 'keys.' One 'public' key and one 'private' key, which are just files that can be stored on a user's computer or USB drive. The user shares his or her 'public' key with others so that they are able to use the key to encrypt a

message they would like to send to the user. The user then uses their 'private' key to decrypt any messages they have received or 'sign' any messages, to verify their identity and reassure the recipient that they are communicating with the intended recipient (Mounteney et al., 2016). Figure 26 shows a message before it has been encrypted and Figure 27 shows a message after it has been encrypted by the PGP code (Mounteney et al., 2016, pg. 45). The message in Figure 27 would be the message that could be viewed if the message was intercepted. PGP is primarily used in cryptomarkets for buyers to send shipping information to sellers. In order for the sellers to send their buyers their package, they must have a name and address (Mounteney et al., 2016).

Some users encrypt their communications even further and utilize hard-drive encryption. This technology protects the user's computer even if law enforcement has their physical computer in hand. A password is needed to decrypt the messages on the hard drive. Some programs even allow users to set up two different passwords to signal to their computer what information they would like to be shown. For example, if the user is under surveillance, they can type in one of their passwords which would only reveal a small portion of their encrypted material, the other password would reveal all of their encrypted material (Mounteney et al., 2016). Most cryptomarkets will provide extensive information on how to create a multi-signature wallet, how to use a PGP key, among many other user tips (Knowledge Base and Support, 2017).

Some sites choose not to sell certain illegal products, and who said there was no honor among thieves? Agora, one of the current most prominent sites on the Dark Web decided they were going to ban the sale of guns, poisons, and fraud products (I am a Tor,

2015). It is speculated that this move may be due to ethical concerns, but most likely, this ban stems from the correlation of the sale of these types of illegal items and being hacked. Government adversaries have a particular interest in actively intercepting these types of goods. The UK and Australian governments, in particular, have been strongly enforcing illegal gun sales law (Leyden, 2015). The Australian government has made a concerted effort to intercept packages containing illegal goods. This deters some Dark Net sites from doing business in and out of Australia, however, many still do, despite the increased risk. Silk Road also banned the sale of “anything whose purpose is to harm or defraud, such as stolen credit cards, assassinations, and weapons of mass destruction” (Chen, 2011, pg. 3) on their site. Figure 28 shows goods that are “Forbidden” on Hansa, these goods include human trafficking, toxins, explosives, and human organs (Forums: Hansa, 2017). Kruithof et al. (2016) found that the most commonly banned listings were child pornography and assassination services. By banning these particular goods, Agora, Silk Road, and other sites like it, are signaling to their customers that they wish to eliminate the probability of getting hacked by independent adversaries or legal adversaries.

5.2.2 Conflict Resolution Services

As noted above, cryptomarket sites settle disputes between users, ban users who are not following the site rules, and structure the site in a way to align user incentives and deter fraud initially. Some sites are more explicit than others about how they will resolve disputes. Kruithof et al. (2016) found that many sites stated that if a seller scammed a customer, it would result in the deactivation of their account. Some sites will not state

this policy explicitly but will leave evidence of their deactivation processes in their forums. Hansa provides very specific information on their dispute resolution process:

What situations call for a dispute?

- If your shipment did not arrive
- If the vendor has sent you the wrong listing
- If your shipment was incomplete or damaged

What does not call for a dispute?

- The quality of a drug is sub-par
- You do not know what to do with information from a guide or e-book.
- You do not know how to open, edit, or handle a digital item.
- Fraud methods from a guide or e-book are outdated.

In these cases, please leave negative feedback for the order, but do not dispute it.

How does HANSA decide who wins a dispute?

Each dispute is examined and investigated as impartially as possible. We do not enter a dispute to determine a winning or losing party. We will try to mediate between you and the vendor, and if someone is clearly at fault, we will make sure that we act accordingly.

Dispute rulings are mostly decided by reviewing the following points:

- The vendors accepted terms.
- Market reputation of both accounts.
- Verifiable statements and accusations.

- The dispute and feedback history of both accounts.

(Knowledge Base and Support, 2017)

These more specific rules are less common, however, the forums on Hansa illustrate that Hansa does follow these procedures, to their users' satisfaction (Forums: Hansa, 2017).

6 Conclusion

Cryptomarkets have become a substantial force in global black market. They have revolutionized the way that illicit goods and services are sold and received as well as the way communication about illicit goods and services takes places. Ross Ulbricht stated that his purpose for starting the Silk Road was to create “an economic simulation to give people a first-hand experience of what it would be like to live in a world without the systematic use of force” (Good Wagon Books, 2017). He did successfully, not only for his own site but for many others, create an environment where users function in a completely self-governing society.

In this paper, I argue that, to overcome the problems that anonymity and a lack of formal enforcement, cryptomarkets provide their users with self-enforcing private governance. This governance aligns the incentives of the buyers and sellers of illicit goods and services to facilitate initial and repeated exchange. Platform providers ensure that their sites resolve conflicts, enforce contracts, and provide club goods such as security services.

The arguments I make in this paper are not confined to the boundaries of the Internet black market. They can also be applied to other marketplaces that enable exchange while keeping their users' identity anonymous. Ashley Madison is one such

marketplace. This website is an online dating site aimed at people seeking an affair (Ashley Madison, 2017). This site seeks to connect users without divulging private information to prying eyes, in this case the prying eyes are not law enforcement, but the user's spouse. The argument I have outlined in this paper follows the same logic as mechanisms keeping this infidelity dating site operational.

Chapter 3: Shadow Markets and Hierarchies: Comparing and Modeling Networks in the Dark Net

1. Introduction

In 2011, a young man by the name of Ross Ulbricht changed the game of illicit goods exchange. He created the first ever website that allows for illicit and anonymous exchange to happen over the Internet. No longer were sellers bound by their personal networks or geographic location. With the introduction of the Internet into direct illicit goods exchange, sellers could vastly expand their customer base to a global audience. They could now reliably exchange goods from the comfort of their home, rather than having to go to the streets. Ulbricht's new forum broke a lot of rules that bound traditional black markets. In our paper, we investigate some of the limitations he surpassed and their consequences.

Before the advent of the Internet black market, illicit markets were characterized by face to face interaction, geographic proximity, and social connections. These features determined the way in which information about buyers, sellers, and the very goods exchanged emerges and circulated. Of course, technological innovation disrupts these underlying conditions, forcing market participants to adopt new institutional arrangements. The Internet black market has created new environments for illegal markets to develop. It is imperative to understand how these market networks transpire

and function in order to understand why some persist and others fail (Jones, 2016; Everton, 2012; Gunaratna, 2006).

Criminal organizations, as detailed by Buchanan (1973), Schelling (1971), Fiorentini and Peltzman (1995), and Leeson and Rogers (2012) result in (i) a tendency towards the monopolization of one or more illicit markets and (ii) the adoption of a vertical organizational structure to both exploit economies of scale and restrict access to the market.

This paper focuses specifically on these characteristics and their manifestation in market networks. We compare the structure of illicit ground networks (that rely on face to face or in person transactions) with the network structure of illicit virtual networks (that exist on the dark web). The purpose of modeling these two different types of illicit markets is to understand the characteristics of the network structure that emerges from the interactions of the agents in each environment, subject to different constraints and to discuss their economic implications. We build upon the existing organized crime and network literatures by analyzing the different market structures that emerge with the same traditional illicit goods and services given different constraints.

We use an agent-based model to simulate the conditions in virtual and ground networks, which allows us to analyze the network structures that emerge. Distributions of degree and betweenness are compared, along with network level measures of density and average path length. Degree tells us the number of connections each agent has while betweenness tells us the number of shortest paths that run through each agent both are node level measures. These measures of network structure allow comparison of network

structure, including monopolization and hierarchy, between a simulated ground drug network and a simulated dark web network. We define hierarchy as a system or organization, with different levels of authority, where groups are ranked in order of authority and central control (Mayntz, 2004). We also look at monopolistic tendencies (Ogus, 2002), which results in fewer prominent sellers dominating the marketplace.

In what follows, we examine the determinants of network structure and hierarchy in the Internet black market relative to traditional black markets. Section 2, includes an overview of the digital marketplace for illicit goods. In Section 3, we frame our argument within the organized crime and network literatures and our hypothesis for what we can expect our network simulation to look like. Section 4 provides testing of our hypothesis with an agent based model. Section 5 concludes.

2. The Digital Marketplace for Illicit Goods

2.1 The Dark Net

In order to understand the Deep Web (also known as the Dark Net), it is important to first define the Surface Web and the Deep Web. The Surface Web is comprised of content on the Internet that can be found using a search engine. If Google, Bing, or Yahoo can find certain information, it exists on the Surface Web. Surface Web information is both accessible and indexed. The Deep Web consists of information that cannot be found using a search engine.

For example, if you buy something online from Amazon using a credit card, this information cannot be accessed via a search engine. Online businesses encrypt this

private information to secure their customer's privacy. Organizations such as public libraries, local governments, and businesses manage the majority of data in the Deep Web (Christin, 2012). Information on the Deep Web is estimated to be hundreds, if not thousands of times larger than information on the Surface Web (Deep Web: A Premier, n.d.). This information is accessible but non-indexed, authorized individuals may access this data, but the public cannot. The Dark Net is a subset of the Deep Web, it contains information that is both restricted and non-indexed. Activity on the Dark Net that has to do with exchange is done using anonymous routing technology (Gaup, 2008).

2.2 Tor: The Onion Router

Tor is a network within which users can search and exchange over the Internet, anonymously. It is a volunteer-operated network that protects the privacy of hundreds of thousands of users daily (*Tor Project*, 2015). Tor enables users to more effectively protect their identity when searching online, avoiding surveillance, circumventing censorship, and bypassing firewalls. The network is decentralized and cannot be shut down from an administrative location. The routing system functions in a diffuse way which prohibits law enforcement's ability to identify specific users (Abbot, 2010). The robustness of its security lies in the diffusion of trust all through the system (Johnson et. al., 2011). Using Tor is not costless, it takes a few extra steps to download and it is extremely slow when making a transaction, relative to surface web sites, because of the encryption and evasion of each transmission being made (Dingledine and Murdoch, 2009).

As an open sourced router, Tor connects users in its network and randomly “bounces its user’s Internet traffic through several other computers to keep it anonymous” (Internet Freedom, 2015). The Tor network is made up of relays, which are publicly-listed nodes in the Tor network that forward traffic on behalf of clients, and that registers itself with the directory authorities (McCoy et. al, 2008; *Tor Metrics*, 2015). There are roughly 3,000 relays in the entire Tor network (*Tor Project*, 2015). A client is a node in the Tor network, typically running on behalf of one user, that routes application connections over a series of relays.

Tor is similar to mix-networks because messages are wrapped in layers of encryption. This encrypted information contains keys of all the intermediate nodes that the information will reach before it reaches its final destination. When the information reaches each node a layer of encryption is lost and the information continues traveling randomly throughout the network, losing layers of encryption as it goes (Gaup, 2008). This network allows for anonymous and untraceable communication because there is no correspondence between incoming and outgoing messages from each node the information travels through (Gaup, 2008).

This technology was originally funded and developed by the United States Navy to “protect intelligence gathering from open sources and to otherwise protect military communications over insecure or public networks” (Syverson, 2013). So there are Tor users who are engaging in legal behavior, as the technology was originally intended, however, the black market on Tor has exploded in size and scope (Johnson et. al., 2013).

2.3 Cryptomarkets

The Internet black market is a widely used group of sites on Tor, this anonymous network, coupled with Bitcoins, allows users to make purchases securely and anonymously over the Internet. These cryptomarkets make hundreds of millions of dollars a year and their operations are continuing to expand (Kruithof et. al., 2016). In January 2016 alone, it is estimated that the cryptomarkets generated a monthly revenue of between \$14.2 million (excluding the sale of alcohol and tobacco) - \$25 million (including all visible listings) (Kruithof et. al., 2016). There have been over 80 platforms that have existed or still do exist on the Internet black market. Some were hacked, raided, scammed or voluntarily shut down and over 20 different platforms are still in operation today (Black Market Risks, 2015).

The Internet black market is an environment that, relative to traditional markets, has less asymmetric information, higher entry costs, and lower transaction costs (Hardy and Norgaard, 2015). Platforms in the Dark Net are able to identify and enforce property rights more effectively due to the ease of contract enforcement, reliability of privacy, trustworthiness of sellers, use of branding, and use of anonymous currency, all of which will be discussed below.

Platform providers can use various code bases to make marketplaces within the dark net, sellers then advertise their goods on these different sites. Some sites are open to anyone, others require a referral (Bakken, 2015). Sellers utilize various techniques in order to attract buyers. The use of logos, community bonding through forums, and reputation through repeated interaction creates a more transparent and user-friendly community (Bakken, 2015). Marketplace administrators play a critical role in dealing

with vendors who scam customers or sabotage each other. Kruithof et al. (2016) presents an analysis of the rules of ten cryptomarkets which keep the markets functioning.

Vendors have explicit dispute resolution procedures to protect their users and prevent fraudulent behavior. Figure 29 shows dispute resolution procedures on Hansa, an Internet dark market site (Knowledge Base, 2017). The platform encourages the buyer and seller to solve the dispute amongst themselves, if this is not possible, Hansa staff follow a delineated resolution procedure. If the dispute is ruled in favor of the buyer, the staff member will force the vendor to compensate the wronged buyer (Knowledge Base, 2017).

Various sites rank their members based on their tenure and the trust they have built up on their site, Figure 30 shows different participants in Silk Road 2 (a specific Dark Net site), and their corresponding site rankings (Bakken, 2015). Customers also rate the vendor's products on a scale from 0 – 5 stars (Dolliver and Kenney, 2016). This rating system allows vendors with high ratings to charge a premium for their products because of their good reputation (Hardy and Norgaard, 2015).

Because Bitcoin is the most popular and widely adopted anonymous crypto currency, it is used as a primary medium of exchange on Tor. A Bitcoin is technically a solution to a mathematical equation with a fixed set of solutions (Grinberg, 2011). This digital currency is able to be stored in a virtual “wallet”, similar to cash, and is exchanged with low transaction fees through anonymous virtual transactions (Briere et. al, 2013). As a peer-to-peer currency, it does not require verification from a central third party (Christin, 2012). Bitcoin uses the Blockchain which is a transparent public ledger

distributed by a peer-to-peer network. This Blockchain technology prevents ‘double spending’ of Bitcoins by certifying that the same Bitcoins haven’t already been used in a transaction (Trautman, 2014). Thus, exchanges made using Bitcoins over the Tor network are extremely difficult, if not impossible, to trace.

Digital, anonymous, drug communities are increasingly innovative in their capacities to retail and market drugs, provide information for users regarding drug sourcing mechanisms, advice around optimal use, and host discussions around popular choices, experiences and harm reduction practices (Wax, 2002; Gordon, Forman, & Siatkowski, 2006; Griffiths, Sedefov, Gallegos & Lopez, 2010; Davey, Schifano, Corazza & Deluca, 2012). Widespread drug product availability is fueled by novel drug trading sites such as ‘Black Market Reloaded’, ‘The Armory’ and the ‘General Store’ (Christin, 2012).

3 Markets and Hierarchies

3.1 Organized crime

The organized crime literature explains the organization and actions of criminal groups in terms of the incentives faced by criminals as rational actors. A universally accepted definition of organized crime has yet to be delineated, thus, there are various illustrations as to what constitutes organized crime. It has been characterized as a long term arrangement, amongst criminals, without state enforcement (Leeson, 2007) and as more of a predatory relationship rather than a voluntary and firm-like exchange (Skaperdas, 2001).

Regardless of the technical definition, however, organized crime is a question of costs and benefits. Criminals decide to interact with one another when they are able to receive higher compensation from organizing rather than acting alone (Chang 2005). The organized crime literature explains the organization and actions of crime groups in terms of the incentives faced by criminals as rational actors.

The model of the rational criminal, developed by Becker (1968), lays the foundation for the literature of organized crime. He applies the basic economic framework of analysis to this peculiar non-traditional market. Schelling (1971) posits that the organizational and network structure that organized criminals seek is one of monopoly or hierarchy without competition. This, he argues, is a defining characteristic of organized crime; “organized crime is usually monopolized crime” (1971, 182). Schelling finds that there is a tendency towards monopolization because of the nature of illicit goods themselves. The exchange of illicit goods results in the potential for violence, thus, organizations form with the ability to exclude outsiders (1971).

Because there is no third party enforcement of criminal contracts, criminals must police themselves, thus tending to band together. The nature of this environment leads to one in which these organized criminals seek exclusive influence and authority of their territory and work to keep other criminal groups from invading. However, Schelling notes that “rival claimants to monopoly position sometimes find it cheaper to merge than to make war” (1971, 645). Therefore, Schelling also concludes, there is a tendency toward monopolization in organized crime settings (Schelling, 1971).

Buchanan (1973) argues that organized crime groups have monopolistic tendencies as well. Because monopolies limit the supply of goods, they are socially desirable in a criminal setting. The equilibrium amount of crime, supplied by a monopoly, is less than the amount of crime supplied by multiple criminal groups (Backhaus, 1979). This is because the purpose of a monopoly has always been to suppress, not enlarge, supply, especially in a criminal setting (Schelling, 1971). Fiorentini and Peltzman (1995) characterize criminal organizations as groups that exploit monopolistic prices on the supply of illegal goods and services and establish a hierarchy that manages risky behavior. Leeson and Rogers (2012) attribute hierarchical criminal organization to market contestability. The lower the entry costs, the more the criminal organization is likely to organize hierarchically. The extent of the hierarchy is that of the current criminal organizations enforcing monopolistic control of the market against potential market entrants (Leeson and Rogers, 2012).

Garoupa (2000) and Dick (1995) emphasize the influence of transaction costs rather than monopoly power in organized crime groups. Transaction costs are the costs of identifying and enforcing property rights (Allen, 1999), something that can be very complex in criminal organizations. Garoupa (2000) argues that transaction costs in underground markets are relatively low but with imperfect information they will be higher. Jennings (1984), likewise, does not emphasize monopolistic behavior in organized crime. Instead, “oath taking”, he posits, is primarily driving organized criminal behavior. The act of committing oneself to a larger organization increases the cost of defection and thus decreases the risk of detection.

A more recent extension of the organized crime literature includes papers in which economic tools have been applied to historical cases of organized crime. These papers are similar to our work in the sense that they apply this lens to natural instances of organized crime. Gambetta (1996) and Varese (2001) find that Mafia groups, The Sicilian and Russian Mafias respectively, emerged in low trust societies as a substitute for formal property rights enforcement. These Mafias had a centralized structure and a permanent and hierarchical organizational arrangement (Gambetta, 1996).

Skarbek, (2010, 2011, 2012) likewise in his research of prison gangs, finds that these criminal organizations emerged to protect inmates, lower transaction costs, and enforce property rights. He finds that “members of the Mexican Mafia and Nuestra Familia established hierarchical organizations with effective information transmission and enforcement mechanisms” (Skarbek, 2012, 39-40). Leeson (2007, 2009, 2010) finds that some criminal organizations are so sophisticated as to have checks and balances in a constitutionally constrained democratic government, Pirates in the 1900s. Piano (2017), in his research of the Hell’s Angels motorcycle club, finds that this criminal organization was successful because of its hierarchical organization. This network structured allowed them to mitigate internal conflict while expanding and profiting from their illegal activities.

The organized crime literature also supports the claim that hierarchy plays a very pivotal role in the network structures of criminal markets and is an appropriate component of analysis (Levitt and Venkatesh, 2000; Piano, 2017). Numerous studies

suggest that criminal organizations are already embedded into preexisting societal hierarchies and thus, have some level of hierarchical structure themselves (Jankowski, 1991; Spergel, 1995; Akerlof and Yellen, 1994). Lazear and Rosen (1981) argue that, because criminals are overwhelmingly risk-loving individuals, there will be a tournament structure of organized crime where there is an incentive for upward mobility. Group members will compete to rise in the ranks of the organizational hierarchy (Lazear and Rosen, 1981).

Although many of these historical criminal organizations have hierarchal organizational structures, there is evidence to suggest that hierarchy impedes underground market transactions amongst criminals. In their study of P.O.W. camps during WWII, Holderness and Pontiff (2012) found that camps with less hierarchy had higher levels of survival and more flourishing markets within the camps.

3.2 Networks and Hierarchy

Networks give us the ability to “bridge the gap between the individual and the population” (Comparing Networks, 2008). The importance of network structures for the transmission of knowledge and the diffusion of technological change has been recently emphasized in economic geography, which our paper takes into account in the ground network and notes the absence of in the virtual network (Broekel, 2014). Network structures are central in driving the innovative and economic performance of actors in regional contexts, and thus, it is crucial to explain how networks form and evolve over

time and how they facilitate inter-organizational learning and knowledge transfer (Broekel, 2014).

Barriers to trade, such as high transaction costs and information asymmetries, limit the quantity of individuals participating in the ground drug network. The removal of said barriers, through the digitalization of the network, drive its expansion. “Networking is giving rise to unprecedented opportunities, facilitating internationalization,” which is what we observe when the illicit drug market is made available via the Internet (Dana, 2001). Comparatively, the technological barriers to entering a digital market are significantly lower than the associated risks of a ground network. Virtual networks are associated with much higher levels of efficiency (Martin, 2014; Buxton and Bingham, 2015) and virtual networks are more likely to provide goods with minimal violence and superior product quality than traditional ground networks (Martin, 2014).

The literature suggests that there are costs and benefits of hierarchy. Less hierarchical networks are more likely to persist because they are less likely to collapse if key players in the network are removed (Arquilla and Ronfeldt, 2001; Jones, 2016). The more diffuse the network is, the more difficult it is to target and disrupt communications between agents (Eilstrup-Sangiovanni and Jones, 2008). However, more centralized network structures are much more effective at carrying out complex tasks in a standardized way (Eilstrup-Sangiovanni and Jones, 2008).

3.3 Hypotheses

Buchanan (1973) and Schelling (1971) suggest that different black markets with different illicit goods for sale will result in varying market structures. We test whether or not we see varying market structures from the sale of the same goods with different constraints. The Internet black market is a network that, relative to illicit ground markets, has higher entry costs and less asymmetric information and lower transaction costs (Garoupa, 2000). We expect information asymmetries to be lower in markets with lower transaction costs. We hypothesize that, given that hierarchy emerges to manage risky behavior (Fiorentini and Peltzman, 1995) and in criminal organizations with low entry costs (Leeson and Rogers, 2012), we will observe a less hierarchical network structure in the Internet black. We also anticipate that we will observe monopolistic market tendencies because monopolistic market tendencies are a feature of markets that deal in illicit goods (Schelling, 1971). Our virtual market network model, will therefore, be less hierarchical and have monopolistic tendencies.

3.4 Preliminary Evidence

In the Internet black market, these crime groups are often organized by type of illicit good or by platform type. Many sites will specialize in a few illicit markets, drugs for example. Agora, one of the longest running and most prominent sites on the Dark Web decided to focus more on the sale of drugs and banned the sale of guns, poisons, and fraudulent IDs (I am a Tor, 2015). Some sites will only allow buyers and sellers who have a referral to exchange on the site, limiting the user base to only experienced users (DeepDotWeb, 2017).

We compare whether different constraints on different illicit drug market places results in more or less hierarchy and monopolization. Figure 11 shows a timeline of Dark Net sites that have existed, or still do exist. Over 80 sites have existed since the birth of the Dark Net in 2011 and over 20 are currently in business. This number of sellers has fallen from over 45 sites in business in 2014 (Darknet Market, 2017). In our model, we compare monopolistic tendencies in the ground market versus the virtual market by analyzing the number of prominent sellers that emerge. We expect monopolistic network structure to be a characteristic of both modeled marketplaces.

Although behavior in the Internet black market is risky, there are fewer information asymmetries, which makes risk, relative to illicit ground markets, lower. Even with surface web exchange, transaction costs are much lower than a traditional marketplace, it gives users access to many more vendors than they are geographically close to. Similarly, in the Internet black market, transaction costs are drastically lower than ground markets. Like these historical cases covered by the literature, we emphasize the importance and prevalence of hierarchy, and analyze how it is different under different constraints.

4 Testing our Hypothesis Using Agent Based Modeling

4.1 Purpose

Schelling (1971) postulates; “in a purely descriptive sense this tendency toward monopolization surely seems to characterize organized crime” (1971, 183), we test this

descriptive claim on different network structures, along with claims that organized crime groups tend to be hierarchical, with empirical evidence and agent-based modeling.

Network analysis paves the way for a deeper understanding of various marketplaces, especially those for which the data is not plentiful. Due to the anonymous nature of the Internet black market, it is virtually impossible to gather data on real-world transactions made between buyers and sellers. Therefore, agent-based modeling provides an appropriate modeling platform from which we can build out the network structures of these two different marketplaces without knowing the specific transactions within them. Agent-based modeling allows us to simulate transactions in these types of marketplaces, using what we know of these markets as our given conditions, and observe the network structure that emerges from numerous interactions among agents.

The model is built using the object oriented modeling package NetLogo. It makes use of the network extension that allows agents to interact on top of an imported or generated network. This agent-based model is a model of two different types of illicit drug markets. The first type of drug market that is modeled as a ground market, a traditional black market, where interactions between agents take place in person and information about an agent's reputation is not perfectly known to potential buyers. The second type of drug market modeled is a virtual drug market, that exists on the Internet, where interactions and exchanges between agents do not take place in person. Attributes about sellers' reputation are salient. The purpose of modeling these two different types of illicit markets is to understand the network structure that emerges from the interactions of the agents in each environment, given the nature of the goods and services. We

specifically look at the monopolistic tendencies of the networks as well as the hierarchical structures that emerge.

Substantive differences in the functioning of these different markets should give rise to different overall network structures. The hallmarks of the ground network are spatial constraints for interaction and limited or imperfect information that agents use to make the decision to engage in trade. The hallmarks of a virtual network are the lack of spatial constraints on agent interaction and "perfect" information made available via the Internet. Agents can use this information to guide their decisions for interaction and exchange. A network analysis and examination of the networks and structures that emerge from both of the networks will be the basis for comparing the functioning of these two types of illicit markets.

4.2 The Mechanics of Agent Based Modeling

In the past, scientific models have been limited in scope and scale by computational constraints. Computer simulations have expanded the potential for scientific models and have allowed them to include more characteristics of realistic systems. Axtell (2000) summarizes three distinct uses of agent based modeling, (i) to process results or provide a Monte Carol analysis of equations that are explicitly soluble, (ii) to shed light on a solution structure when mathematical models can be written down but not solved, (iii) to explore interactive processes systematically. Our model focuses primarily on use (iii) because we analyze the outcome of agent interactions in two different networks. Agent based modeling, in particular, is a type of modeling that includes a system's individual characteristics and unique behaviors (Railsback and

Grimm, 2012). Agent based modeling allows us to model individual agents with unique constraints and endowments, unlike historical models which often look at the state as an entire homogeneous entity. Each “agent” is like a person in an artificial society. Agents have unique behavioral rules and are given different internal states. Some of these states are variable, while others are constant for the agent’s life (Epstein and Axtell, 1996).

The hallmark of agent based modeling uses object oriented programming that creates agents that are purposeful, heterogeneous, and interacting. Our model uses NetLogo, a package specifically designed for building, visualizing, and experimenting on agent based models. Other commonly used object oriented modeling packages that are used for agent based modeling include MASON, AgentSheets, Repast, and Mesa. This type of programming enables the agents to be purposeful and to interact in a given environment. It focuses specifically on the objects, their constraints, and their resulting interactions (Downey, 2012).

A unique component of agent based models is that they can represent the model visually⁶. Not only is the code working behind the scenes to calculate the outputs from the interactions of the agents, the visual component of the model allows us to see the interaction that is happening. The software package has various types of functionality, the model, the view, and the controller. The model, also known as the code, includes the agent’s endowment and utility function, or in programming terms, data fields and

⁶ Visual representation is not necessary but can be useful for detecting bugs in the code and building intuition

procedures. The view, or the visual part of the interface, visually represents what is happening in the model to the user. We can interact with and change the parameters of the model using the control, or the interactive part of the interface. The controller allows the user to change parameters in the model, before running the simulation, without changing the code (Scott and Koehler, 2011).

In the model, agents and environments are implemented as objects. Objects are agent frameworks that include data about the agent and the environment and procedures (Epstein and Axtell, 1996, pg. 5). Agent behavior is governed by data fields and procedures. The data fields, also known as instance variables, dictate the agent's internal characteristics (ex: age, gender, endowment). The highlighted portion of Figure 31 shows a data field that agents are instantiated with in our model. This code shows that each agent is given a reputation, reputation is randomly normally distributed throughout the agents, with a mean of 4.82 and a standard deviation of 0.63. Each agent also has a given number of comments, the number of comments is normally distributed throughout the agents with a mean of 106 and a standard deviation of 118.

The agent's behavior is governed by procedures, also known as methods. In NetLogo, procedures, such as commands and reporters, dictate what an agent can and cannot do. These are rules dictate how the agents interact with each other and with their environment. For example, the command "let" declares a temporary variables, and the command "set" declares a global variable. Agent procedures include combat rules, mating rules, and trading rules (Epstein and Axtell, 1996, pg. 5). Our model includes

excerpts from our trading rules; the highlighted portion of Figure 32 shows a specific agent procedure. This procedure dictates that the agent will buy more drugs in the virtual network only if the ratio of their stock to consumption is less than their tolerance. The highlighted line of code in Figure 33 shows a procedure where agents in the ground network are only allowed to trade with agents that are within their specific geographic area radius, as dictated by their sophistication.

b.1. Our Model

We first define the parameters that belong to our agents, which is shown in Figure 34. By defining our agents this way, we have dictated which variables, in bold (descriptive notes follow the semicolon), they have access to in the model. Some of these variables are used in both the ground and virtual networks, others, like imperfect-reputation and agents-in-radius, are only used in the ground model. This is due to the fact that agents in the ground model are subject to different constraints. Agents in the ground model have spatially explicit rules that are part of the determination of the other agents they exchange with in the market place. The sophistication of the agent is a proxy for the agents' knowledge of the market around them. More sophisticated agents will generally have more possible connections than they can make with others. The agents in the virtual network, have equal access to other agents in the network. The Internet allows them costless connection with others, without geographic limitations.

In the code shown in Figure 35, we instantiate our agents, in the virtual network, with data fields and give them specific procedures. In the virtual network, our agents are

set with data fields reputation, comments, tolerance, and risk aversion. This portion of our model sets up agents, according to the characteristics of the Internet black market. Sellers in the Internet black market have a reputation, as indicated by a star rating from 0 – 5, and buyers can see how many comments have been left. We include these components in our model by setting reputation up as a random variable, subject to the mean and standard deviation of the data we collected from the Silk Road 2 website. Buyers and sellers each have a stock of drugs and an amount of drugs that they consume. We simulate this with the variables stock and consumption. Agents seek a greater stock of drugs if the amount they have is below their tolerance level, indicated by the variable tolerance. Time, in our simulation, passes in discrete moments which are called “ticks” (Programming Guide, 2017). We “reset-ticks” before each network simulation, meaning each time the simulation is run, the agents have no memory of previously run simulations in either network.

The code in Figure 36 is how we instantiate our agents with data fields in the ground network. Agents in the ground network do not have the comments data field because reputation is a latent variable. Buyers and sellers in traditional ground marketplaces have reputations, however, they are not designated by a specific number, they are a noisy variable that is only imperfectly perceived. They also have a certain level of stock, consumption, and tolerance.

The agent’s procedures on whether or not to buy drugs in the virtual network are shown in Figure 37 and in the ground network in Figure 38. These procedures dictate the

buying behavior of agents on the Internet, as dictated by how buyers and sellers do business in the Internet black market. At every “tick,” agents consume drugs and decide whether or not to buy drugs. First, the activated agent asks itself whether or not the “if” statement holds, is stock/consumption $<$ tolerance? If the answer is yes, the agent becomes a buyer, and all other agents become possible sellers. Every agent is deciding if they can sell drugs. The stock after sale is what every agent has left after a sale. If that number is greater than their tolerance, they can become a seller, which is when they set their internal variable “dealer 1” to true.

Agent’s buying amount is calculated by their consumption times a number (one from a normal distribution, with a mean of 5 and a standard deviation of 1). This information about the buying amount relative to each user’s consumption was calculated from the parsed Silk Road 2 data (Hardy and Norgaard, 2015). They will also “ask” other agents how risky they are, if the agent is a high risk seller, depending on the agent’s risk aversion, the agent might not engage in a transaction. Risk is randomly distributed among the agents. If you are risk neutral, you don’t discriminate against other risky agents. Virtual agents also discriminate against other agents on the basis of their reputation and number of comments. They will then make a transaction with the agent, who is within their risk threshold, who has the maximum number of comments and the highest reputation.

Agents in the ground network, likewise, are subject to certain commands for their market interactions. In the ground network agents are limited to interacting with accents

in their own radius (geographic location). Ground network agents also don't discriminate against other agents based on comments because there are no comments in the ground network and reputation is imperfect. Once agents decide that they will engage in exchange with another agent, a network connection is made.

b.2. Model Visuals

The controller enables us to switch between the virtual network and the ground network as well as set the number of agents, risk threshold (between 0 and 5), average rate of consumption (between .1 and 1), and sophistication (between 0 and 5). Figure 39 shows the controller set up for the virtual network and the corresponding view.

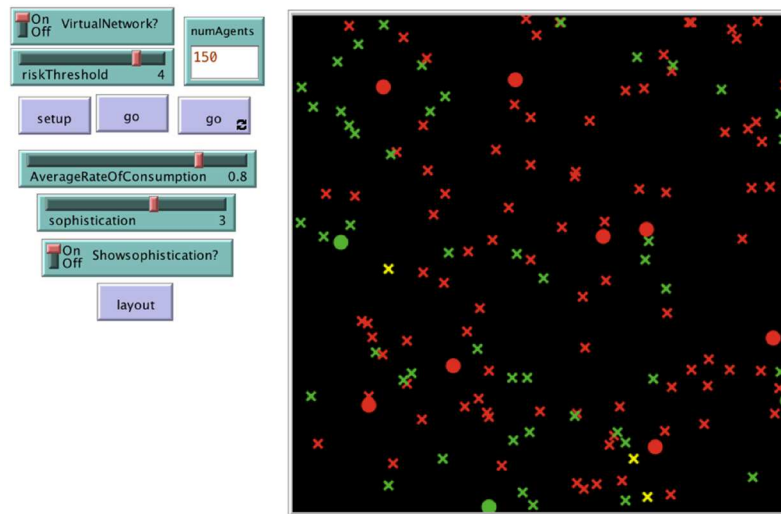


Figure 39 Controller Set up for Virtual Network

There are 150 agents in this simulation with a risk threshold of 4, average rate of consumption 0.8, and a sophistication of 3. After running the model, we can see the connections that each agent has made, delineated by a line between them, and the prominent sellers and buyers that have emerged. Figure 40 shows the outcomes of the model, once it has run. The interface also includes outcome variables from the model simulation; sum of stock, mean sophistication, mean consumption, mean agents in vision, a chart that tracks the number of transactions over the run of the model, and transaction ratio.

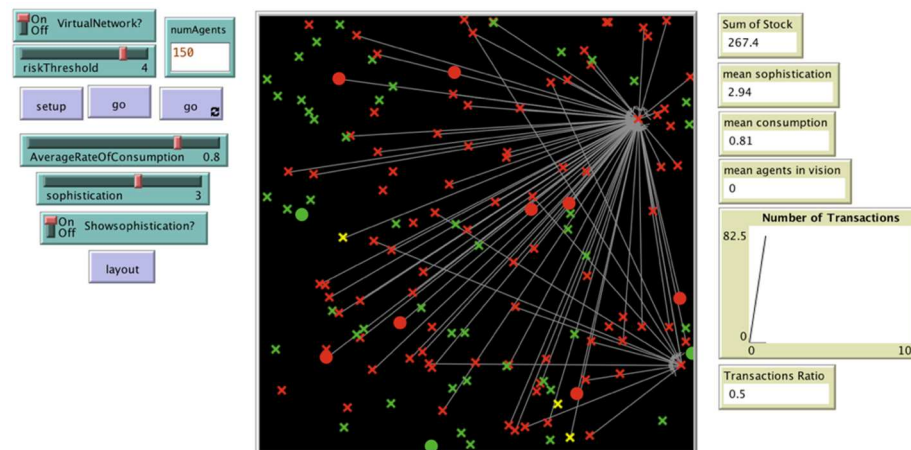


Figure 40 Virtual Model Outcomes

Figure 41 shows the same output with a different layout, as invoked by the layout button on the interface.

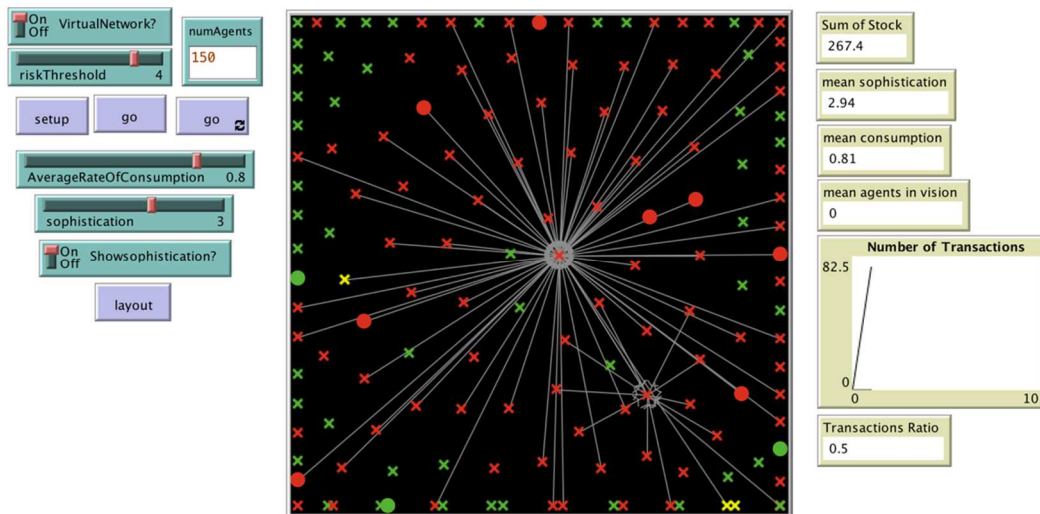


Figure 41 Virtual Model Outcomes Formatted

The same simulation parameters are set in the ground network, as shown in Figure 42.

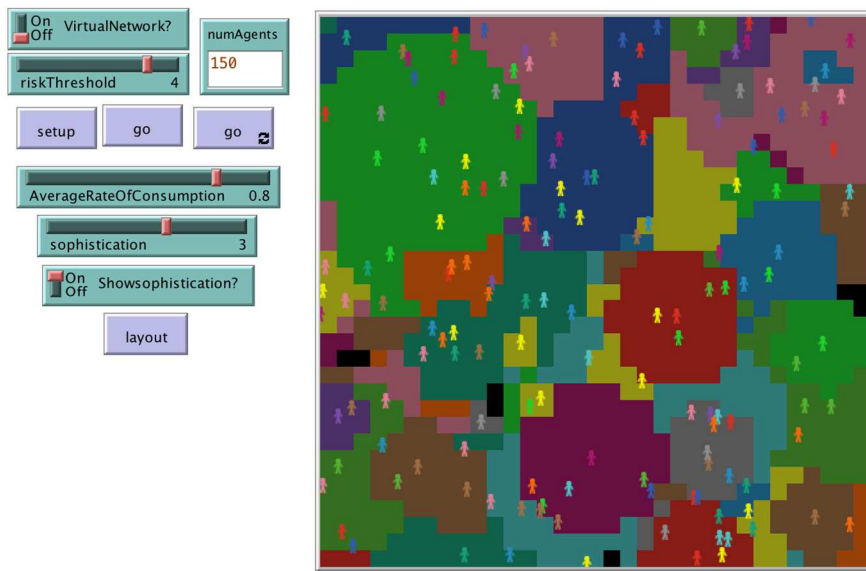


Figure 42 Controller Set up for Ground Network

Figure 43 shows the network connections agents in the ground network made after the simulation was run. There are many fewer network connections made in the ground network versus the virtual network with these parameters because of their geographic trading constraints. The layout feature, which allows network connections to be seen more clearly, is used in Figure 44.

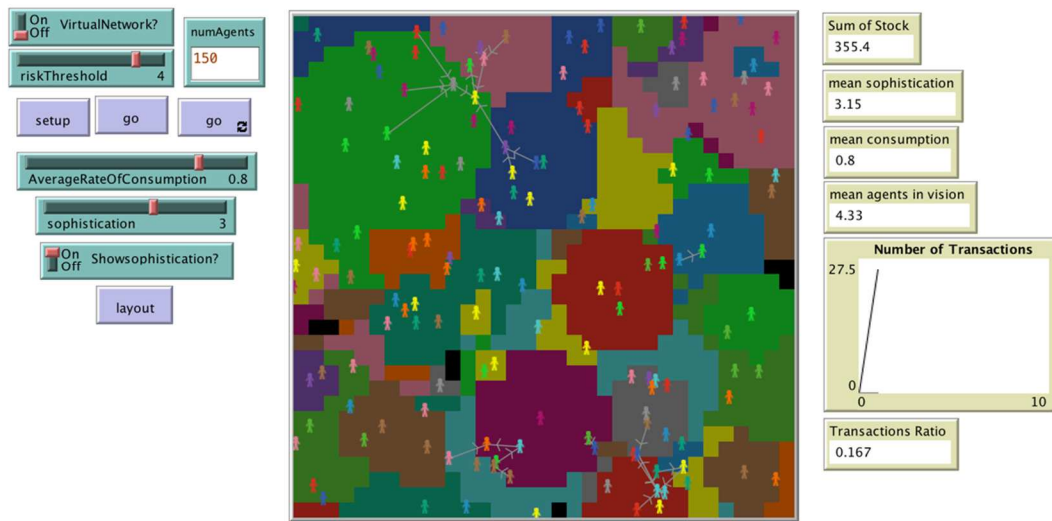


Figure 43 Ground Model Outcomes

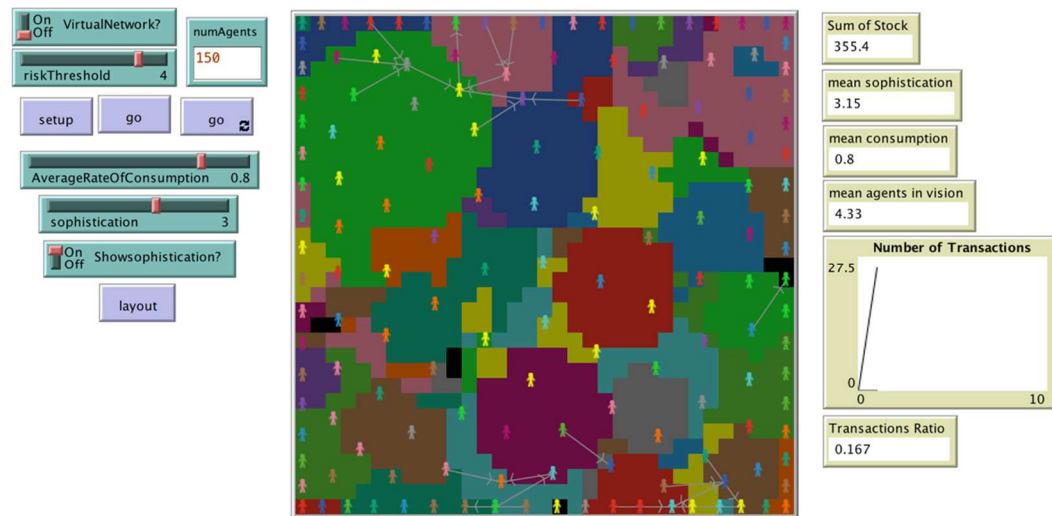


Figure 44 Ground Model Outcomes Formatted

We connected the programming language R to NetLogo to conduct a series of parameter sweeps on both the virtual and ground models. We ran each simulation 100 times at each of the five levels of sophistication, 1, 2, 3, 4, and 5. The metrics, holding all others constant, we collected include; average path length, average degree, average betweenness, average network density, the number of weekly and strongly connected components of a graph, and the average percent of the total transactions that could have happened in the model.

4.3 Entities, State Variables, and Scales

The ground model and the virtual model consist of agents that are able to both consume and acquire drugs. In the ground model the agents exist on a two dimensional spatial landscape. The virtual model does not include this spatial dimension because the agents can be located anywhere and they use a virtual network (i.e. the Internet) in order to interact and engage in exchange. The agents in both models share many of the same attributes like the types of goods and agent reputation; however, there are also attributes that are unique to each model. These differing attributes provide us the variation in our analysis in order to compare the two different emergent network structures.

Reputation is an agent attribute common to both models. It is empirically derived from Deep Web data (Hardy & Norgaard, 2015) and in the model represents the true reputation of each agent. Reputation is included in the model because “[it] is crucial...as a signal to other users that they are honest and credible individuals. This signal works to differentiate between honest and dishonest users to ensure that honest users are not driven out of the marketplace by dishonest users that are not properly identified” (Hardy &

Norgaard, 2015). It is a latent variable in the ground model because one of the hallmarks of the ground model is imperfect or incomplete information. Reputation is a salient attribute in the virtual model because all agents are able to use the Internet to view the derived reputation of every other agent. In virtual markets users have strictly more information about sellers, including information about lack of reputation, than those in ground markets.

Imperfect reputation is an agent attribute unique to the ground model. An agent's imperfect reputation is based on the true reputation assigned to them based on the empirical distribution of the Deep Web data. It is normally distributed around the agent's true reputation and represents an agent's imperfect perception of another agent's reputation.

An agent's sophistication is an agent attribute that is normally distributed around the average sophistication specified in the model. In both the ground and virtual models it represents a latent variable that encapsulates information about an agent's involvement in the market, specifically is it correlated with the stock of drugs with which each agent is instantiated. In both models, stock is an agent attribute that is normally distributed around an agent's sophistication. In the ground model, sophistication is also correlated with how far each agent can see around their unique spatial environment and consequentially, it determines what other agents with whom they can interact. An agent's vision specifies the other agents with which she may interact with, based on location

Consumption is an agent attribute for the amount of drugs an agent consumes each time they use drugs. It is normally distributed around the average rate of consumption specified in the model. Tolerance is another agent attribute for the number of "doses" of a drug an agent wants to have available to them. It is a threshold value above which an agent will not feel the need to acquire more drugs but that below the threshold would cause them to make the decision to search for and acquire more drugs.

Comments is an agent attribute that is unique to the virtual model. It is empirically derived from Deep Web data (Hardy & Norgaard, 2015) and represents the number of comments an agent has received on their virtual seller profile. The number of comments are included as a property on the agents because "Due to the anonymity aspects of The Silk Road, buyer information is not formally posted like seller information and feedback is on the site. Unlike Surface Web marketplaces like Amazon or EBay, if a buyer leaves a comment and/or rating, an individual identifier is not attached to their message. The reason for this is to protect buyer anonymity. The only information that we can glean about the buyer in particular is that the Silk Road site has confirmed that that particular buyer did make a purchase from a particular seller. Therefore, buyers cannot leave comments on seller's pages from which they did not buy a product (Hardy & Norgaard, 2015). Comments is a salient attribute in the virtual model because all agents are able to use the virtual network to view the number of comments of every other agent when making their decision to acquire more drugs.

There are two agents' attributes that are unique to the virtual network and that deal with the risk preferences of the buying agent and the riskiness of a selling agent.

Risk is an attribute noting if the buyer is risk loving, risk averse or risk neutral. This variable is assigned based on a survey conducted by Gallup (2014) that quantified the distribution of investors that were risk-loving, risk-averse or risk-neutral. The variable for high risk seller is a flag that denotes whether or not an agent's reputation falls above or below the risk threshold specified as a global variable in the model.

4.4 Process Overview and Scheduling

Each step of the model a random activation scheme is used to make the total number of agents in the model become active. Each one of these agents uses drugs (i.e. buyers can be sellers and sellers can be buyers) and this is in line with the findings of Van Hout & Bingham (2014) write; “vendors described themselves as ‘intelligent and responsible’ consumers of drugs. Decisions to commence vending operations on the site centered on simplicity in setting up vendor accounts, and opportunity to operate within a low risk, high traffic, high mark-up, secure and anonymous Dark Web infrastructure. The embedded online culture of harm reduction ethos appealed to them in terms of the responsible vending and use of personally tested high quality products.” In both models the agents continue to engage in transactions as their individual stock and overall stock decreases. Individual agents are allowed to have a “negative stock” of drugs. This results from many agents wanting to buy drugs from the same supplier. After a tick of the model where a popular selling agents supply drops below its tolerance threshold they will no longer be included in the list of possible sellers that other agents in the model can buy from. This is model where the agents are endowed with a certain stock of drugs at the beginning and never have their stock replenished by some outside supplied of drugs.

This aspect of drug market models is outside the scope of this paper but could be a rich area for further research and modeling. The model continues to run until the total stock of drugs falls to zero or below.

4.5 Process Overview of Ground Model

The ground model is a spatially explicit model that is setup by assigning each agent a random position on a 2D x-y plane. Agents can only interact with other agents that are within their own-vision. At each tick of the model, every agent reduces their stock of drugs by the amount of their consumption. After this each agent checks to see if the number of "doses" they have left is less than their tolerance. This is done by subtracting their consumption from their current stock to arrive at the number of "doses" they have remaining. If this number is less than their tolerance they will decide to buy more drugs. The amount that the buying agent wants to buy is normally distributed around five meaning that on average whenever an agent buys drugs they are buying five doses of drugs. The buying agent creates an agent set (called possible-sellers) of the agents that are within their own-vision and that have enough drugs to sell such that the selling of their drugs will not cause their number of doses left to fall below their tolerance. The agents that don't meet this criterion are thrown out of the possible-sellers agent set. The remaining possible-sellers set their variable called imperfect-reputation according to a standard normal distribution that is centered on their actual reputation. The buying agent then picks the seller with the highest imperfectly perceived reputation and this agent becomes the final dealer. A link is made with the final dealer and the final

dealer has their stock reduced by the buying amount and the buying agent has their stock increased by the buying amount.

4.6 Process Overview of Virtual Model

The virtual model is not spatially explicit and is setup by instantiating the agents with their own reputation, number of comments and their risk and risk aversion. At each tick of the model every agent reduces their stock of drugs by the amount of their consumption. Agents then divide their current stock by their consumption to arrive at the number of “doses” they have remaining. This is then checked against their tolerance: if his number is less than their tolerance they will decide to buy more drugs. The amount that the buying agent wants to buy is normally distributed around five meaning that on average whenever an agent buys drugs they are buying five doses of drugs. The buying agent is able to view every other agent in the simulation and creates an agent set of those agents (called possible-sellers) that have enough drugs to sell such that their selling of their drugs will not cause their number of doses left to fall below their tolerance. If the buying agent is risk averse they limit the existing possible sellers to those that are low risk and if the buying agent is risk loving, then they limit the existing possible sellers to those sellers that are high risk. If they are risk neutral then there is no change to the existing set of possible sellers. At this point the buying agent looks at the number of comments each possible seller has and limits their choices to those agents with the higher numbers of comments. The agent with the highest reputation in this group is selected as the final dealer. A link is made with the final dealer and the final dealer has their stock

reduced by the buying amount and the buying agent has their stock increased by the buying amount.

4.7 Design Concepts

4.7.1 Basic Principles and Emergence

The ground network is a spatially explicit model with limited and imperfect information. In the virtual network agents are not constrained by space and they have access to the "perfect" information of the Internet black market. There should be a fundamental difference between the networks that emerge from a traditional ground network and a virtual Internet black market. These might include the visual structure of the network, distributions of centrality measures, clustering and modularity, and path length. The networks that emerge will be able to be compared to each other along these measures and at different levels of parameters from the parameter sweep.

4.7.2 Adaption and Objectives

When an agent's supply of drugs falls below their internal tolerance they make the decision to engage in a search for drugs. One model allows this search to take place in a more traditional ground environment while the other model allows this search to take place virtually. Both models have the agents engage in indirect objective-seeking behavior. Buying agents in the virtual model pick selling agents that have the highest reputation, the desired risk profile and the higher numbers of comments. Buying agents in the ground model can only imperfectly perceive the true reputation of the agents they could possibly deal with and have to make a buying decision based on this information.

The objective in both models is to find a seller that is going to be more "trustworthy". This objective supports Hardy & Norgaard (2015), "the seller feedback mechanisms of readily observable ratings, comments, and thus reputation fit these criteria and are likely to send a fairly strong signal that the seller is honest or dishonest. It would be conceivable difficult for a repeatedly dishonest seller to trick its buyers to leave positive reviews and ratings even though the products and services were a sham. On the other hand, if an honest seller provides their customer's with quality products in a timely manner, it will be relatively easy to receive truthful positive reviews about the seller's quality performance. This dovetails very nicely with what we know about the Silk Road community from studying Silk Road forums in the sense that the community is very active at giving feedback to ensure the safety of its users. These criteria, easily observable signaling and costly signaling for cheaters, do not necessarily apply to the buyers in this marketplace. This failure of buyer feedback to meet the strong signal criteria proposes that buyer signals could contain a great deal of noise and potential for misread signals."

4.7.3 Sensing, Interaction and Stochasticity

Agents in the virtual network do not interact with their environment at all. Agents in the ground network are able to see a certain distance around them and are able to interact with the agents located in this radius of vision. There are no environmental variables that affect the agents or their decisions. The global variables of sophistication and average rate of consumption are used in both the ground and virtual networks to set each agents own-sophistication and unique consumption, respectively. Risk threshold is

a global variable that only affects agents in the virtual network and is used to determine whether a seller is a high risk seller or a low risk seller. All agents in both models can perfectly sense the variables needed to make decisions except for reputation in the ground model which is a latent variable that agents are only able to imperfectly perceive.

Networks are created and emerge from the transactions that agents engage in during the process of acquiring more drugs. The ground network is spatially explicit and therefore interaction between agents at different geographic locations becomes less likely as these agents are farther apart. The virtual network allows all agents to engage with all other agents in the simulation.

Several variables are assigned based on empirically derived data. Because every agent in an agent-based model is heterogeneous they must be distributed and this is done based on a normal distribution with a mean and standard deviation based on the empirical data. The attributes created in the way are reputation and comments. The agent attributes of own-sophistication, imperfect-reputation, stock, consumption and tolerance are assigned according to a normal distribution.

4.7.4 Collectives and Observation

Social networks representing the transactions between agents emerge as the model is run. These networks are un-weighted, directed networks where the link goes from the buying agent to the selling agent. The emergent networks can be extracted from the model using the GraphML format for graphs and analyzed using visual inspection and

network analysis measures such as the distributions of centrality measures, clustering and modularity, and path length.

4.8 Results

A casual visual inspection of the directed networks that emerge from the interactions that take place inside the Virtual and Ground models reveal two very different network structures. Graphs 1 and 2 show examples of the networks that emerge from the Virtual and Ground models, respectively⁷. Both models were run using a value of 3 for the sophistication parameter and an average rate of consumption equal to 0.4. The risk threshold, which is unique to the Virtual model, was set at 4.19. Nodes are colored on the agent attribute of reputation.

⁷ These graphs were created from the outcomes of the model in NetLogo using Gephi, a network analysis and visualization tool.

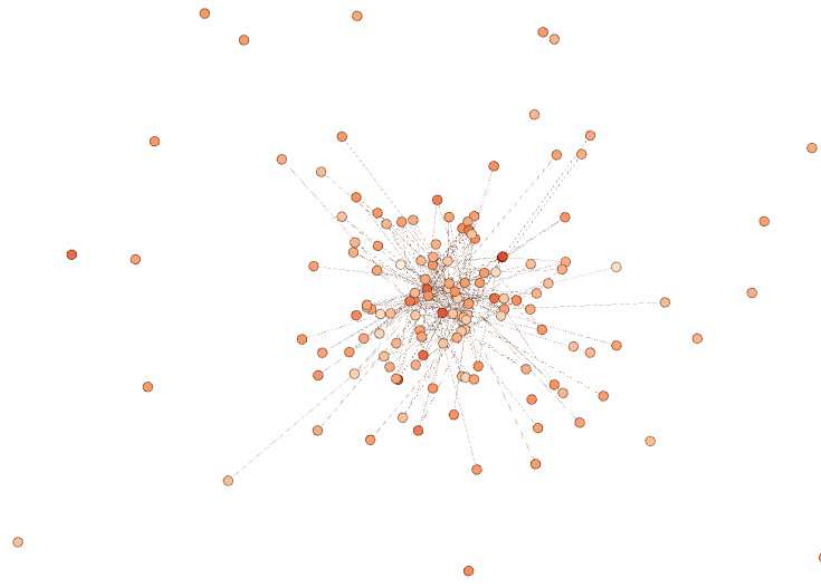


Figure 45 Network structure of Virtual network (Average Degree: 2.03, Density: 0.014)

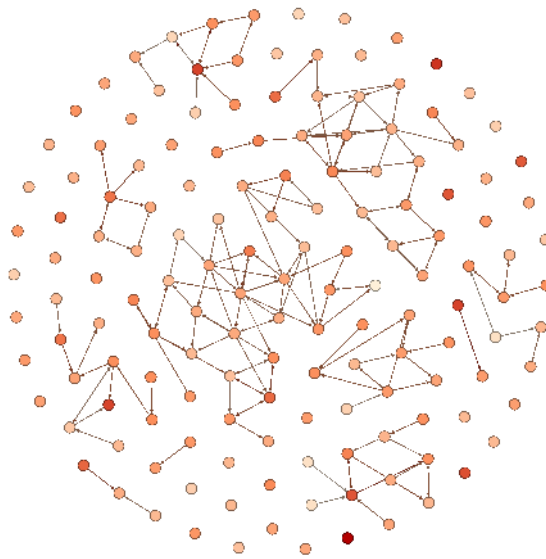


Figure 46 Network structure of Ground network (Average Degree: 1.17, Density: 0.008)

From these views, it is evident that the network structures that emerge in these two different markets are quite different. We observe a much more monopolistic looking network structure in the virtual network, almost a “winner-take-all” monopolistic structure. This is evident by the dense clustering and “hub and spoke” patterns that are prevalent in the virtual network, relative to the ground network.

A series of parameter sweeps were conducted on both the virtual and ground models. The global parameter called “sophistication” was swept at five different levels in both models and each time the simulation was run a total of 100 times. The metrics used to compare the two models are the following: average path length, average degree, average betweenness, average network density, the number of weekly and strongly connected components of a graph, and the average percent of the total transactions that could have happened in the model.

Average path length will give us some idea about the number of agents you would have to go through in order to get in touch with another random agent. Longer average paths would suggest that it is more difficult to reach out to another agent in the network. A lower average path suggests the network is less hierarchical because each agent has to go through fewer levels of rank to reach another agent. Shorter average path length can also suggest more monopolization. If the buyers have fewer options of who to buy their goods from, they will have fewer agents to connect through to reach the monopolistic seller.

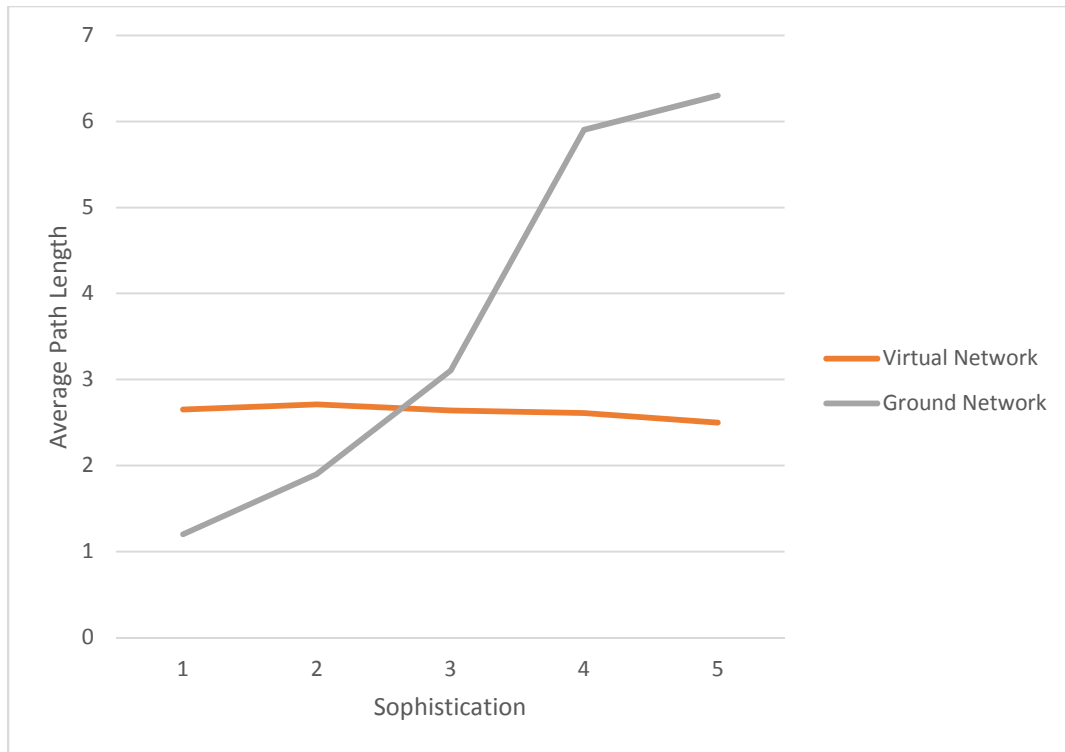


Figure 47 Average Path Length in Virtual and Ground Networks after 100 runs

Figure 47 shows that the average path length, at all levels of sophistication in the virtual network, is between 2.5 and 2.7. This is much less and more concentrated than the average path length of the ground network, that ranges from 1 – 6. This means that, when assigned another random agent, an agent in the virtual network would have to go through less than three other agents to reach them. The virtual network is less hierarchical than the ground network according to this measurement.

Degree, betweenness and network density are all standard measures in network analysis that will give us an idea about how central and connected the agents in the

network are. Degree and betweenness are node level measures. Degree tells us the number of connections each agent has while betweenness tells us the number of shortest paths that run through each agent. Density is a network level measure and tells us the portion of possible connections in a network that are actually connections. Average degree tells us the average number of connections that an agent has and this metric is reported at all five levels of sophistication. Average betweenness tells us the average number of times an agent acts as a bridge between two other agents. Average Density gives us the average density of the networks at each level of sophistication after the running the model 100 times.

Figure 48 shows the average degree in the virtual and ground networks, respectively. Average degree in the virtual network ranges from 3.5 – 5, depending on the sophistication, whereas it ranges from 0-6 in the ground network. It is very difficult for agents in the ground network to make any connections if they have low levels of sophistication because of their prohibitively high transaction costs. Although average degree changes slightly, on average agents in the virtual network, on average, have more connections than agents in the ground network. This suggests the virtual network promotes more peer to peer exchange, rather than going through middle men to buy a product. By this measure, we also observe evidence of monopolization. Because of their market characteristics, transaction costs in cryptomarkets are very low. It is costless for an agent to buy goods from a seller with a 5.0 star reputation rather than from a seller with a 4.9 star reputation. This leads to the emergence of dominant sellers who are highly connected to many buyers. This measure of average degree reflects the large

number of connections that each prominent seller has, relative to sellers in the ground network.

The average betweenness in the virtual and ground networks is shown in Figure 49. Betweenness is a measure of middlemen. In the virtual network, agents act as a bridge between two other agents between 25 and 38 times, depending on the sophistication. In the ground network, this number is between 0 and 600 times. This network measure demonstrates how much more direct exchange there is in the virtual network versus the ground network. The virtual network is much more diffuse and less hierarchical, according to this measure.

Figure 50 shows the average density in the virtual and ground networks. Higher levels of density suggest more monopolization. With lower transaction costs, sellers are able to increase the ratio of connections to possible connections. Fewer sellers are able to connect with more buyers due to their market prominence. In the virtual network, density ranges from .012 to .016, relative to sophistication levels that range from 1 – 5. The density of the ground network ranges from 0 to .020. Only at sophistication levels 4 and 5, is the density somewhat higher than the virtual network. The virtual network is much more consistently dense, suggesting that it has more monopolization tendencies than the ground network. The virtual network is much more consistently dense, regardless of the sophistication, suggesting that it has more monopolization tendencies than the ground network.

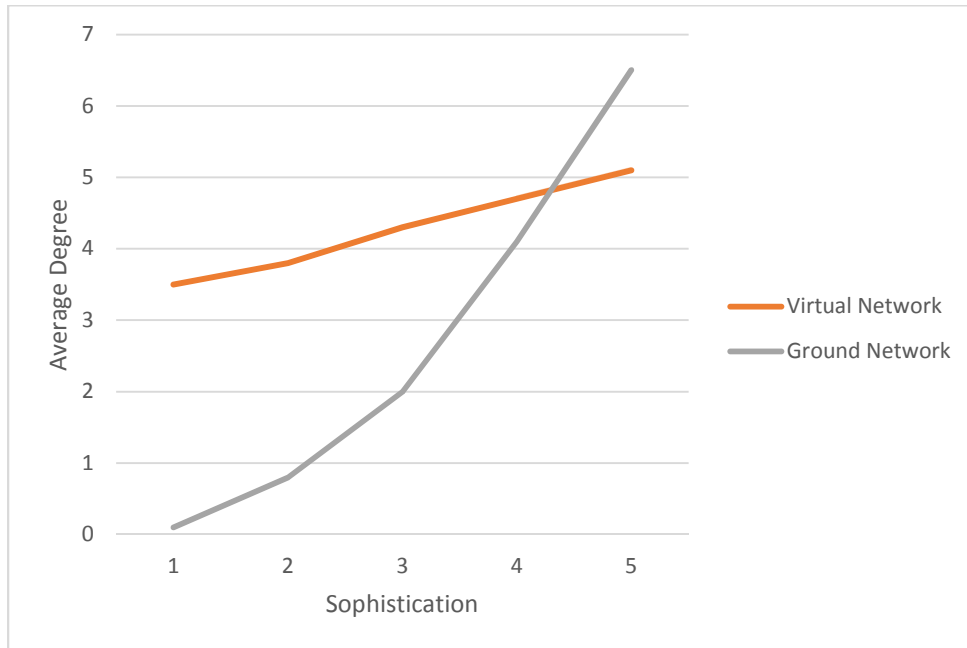


Figure 48 Average Degree in Virtual and Ground Networks after 100 runs

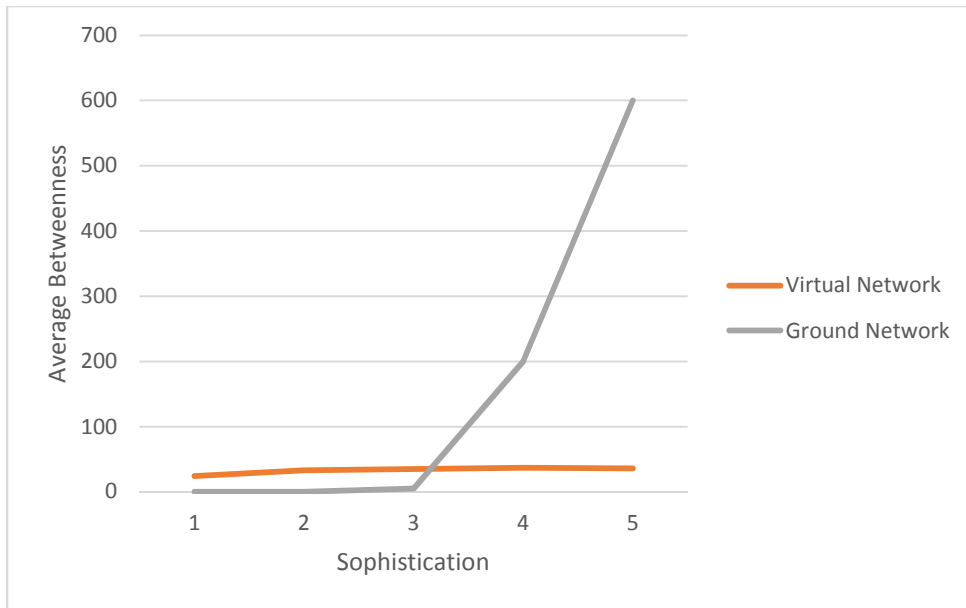


Figure 49 Average Betweenness in Virtual and Ground Networks after 100 runs

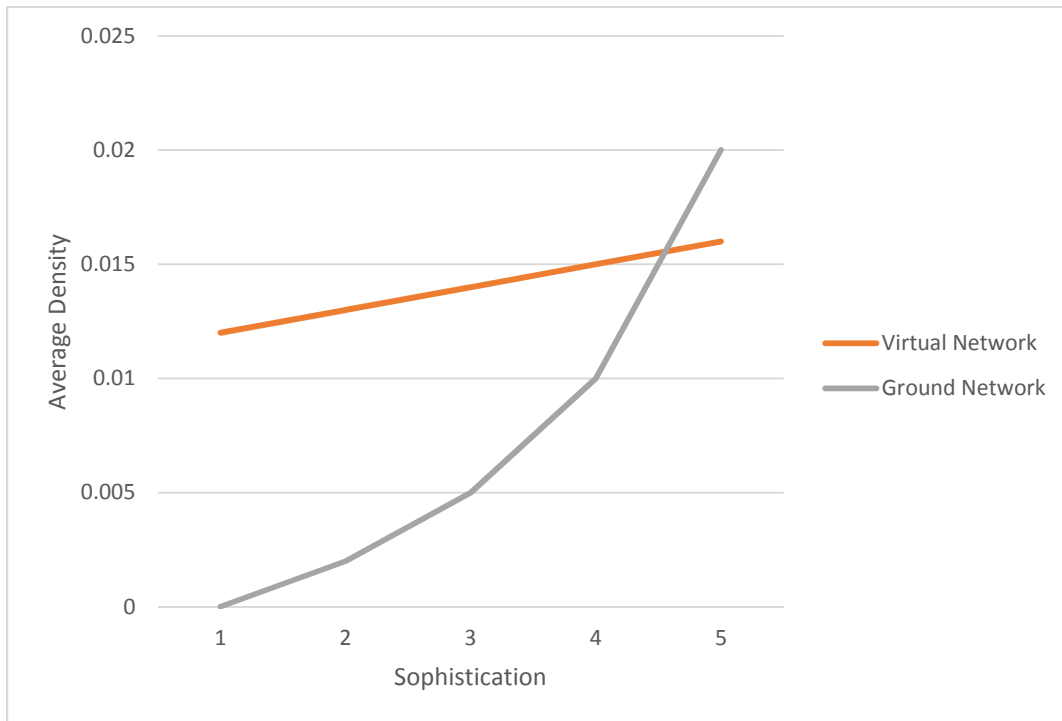


Figure 50 Average Network Density in Virtual and Ground Networks after 100 runs

The number of strongly and weakly connected components tell us about how well connected a network is. A subgraph (a component of a larger graph) is strongly connected if every vertex (agents in the case of this agent-based model) is reachable from every other vertex. Figures 51 and 52 show the average number of strongly and weakly connected components at five different levels of sophistication for both the virtual and ground models. The more “strong” clusters a network has, the more monopolistic it is. Each agent has fewer options and the connections they do have are very strong. Each agent has fewer options of who to connect with and the connections they do have are very strong. Visually this is manifested by the “hub and spoke” pattern we see in the virtual network. Each of these strong clusters is loosely connected with any other strong clusters, suggesting that the buyers in that cluster have found it less costly to interact with fewer sellers in the virtual network.

The greater the number of “weak” clusters, typically the more competitive a network is. We observe that the virtual network has between 120-134 strong clusters and 26 – 37 weak clusters, at various levels of sophistication. Whereas the ground network has 40 – 140 strong clusters and 0 – 130 weak clusters. This measurement demonstrates that virtual networks tend to be more monopolistic at various levels of sophistication and ground networks tend to be less monopolistic.

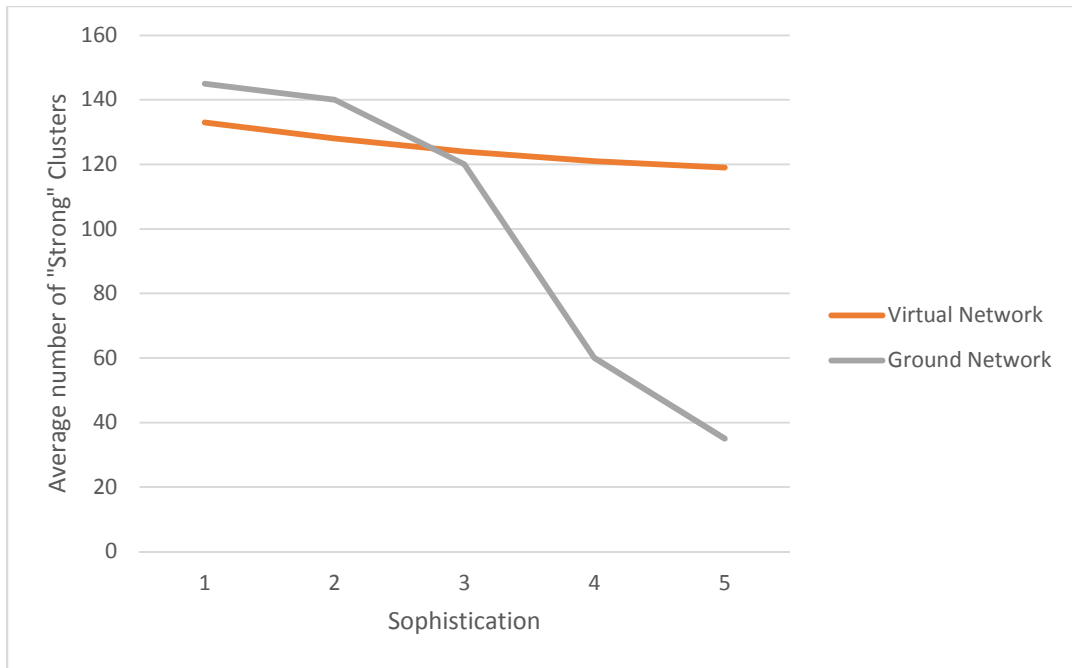


Figure 51 Average number of "strong" clusters in Virtual and Ground Networks

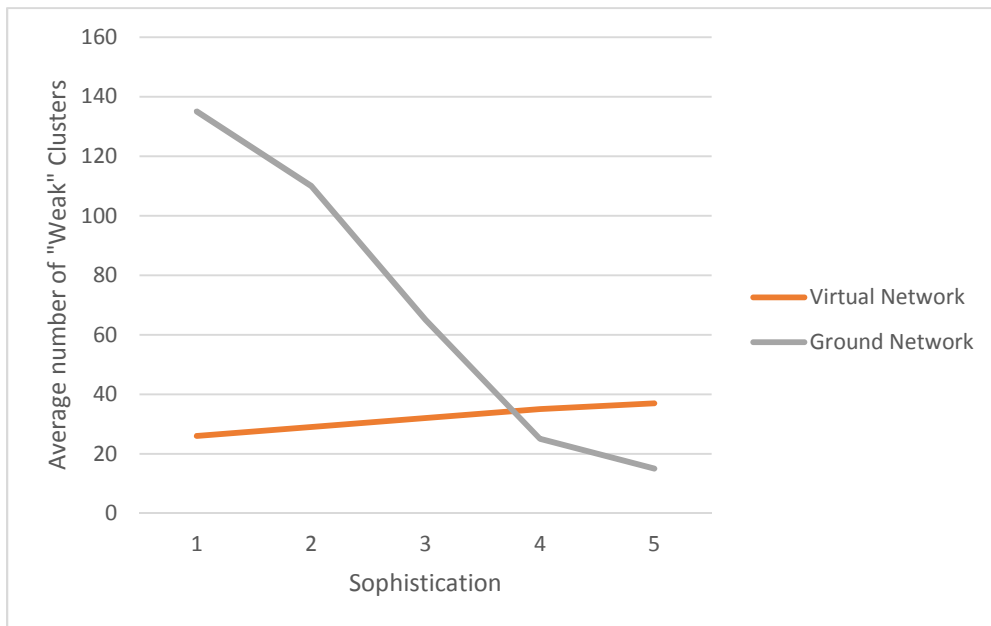


Figure 52 Average number of "weak" clusters in Virtual and Ground Networks

The only non-network measure that is drawn from the models and analyzed is the percent of transactions that actually took place in the model. This metric is defined as the number of transactions divided by the number of possible transactions. More exchange will take place if there are lower transaction costs. It tells us the level of activity inside the model. Figure 53 shows the average percent of transactions that took place at each level of sophistication. The average percent of possible transactions in the virtual network ranged from 22% - 40%, and in the ground network they ranged from 4% - 30%. We observe many more possible transactions taking place in the virtual network because of the overall lower transaction costs and increased information availability.

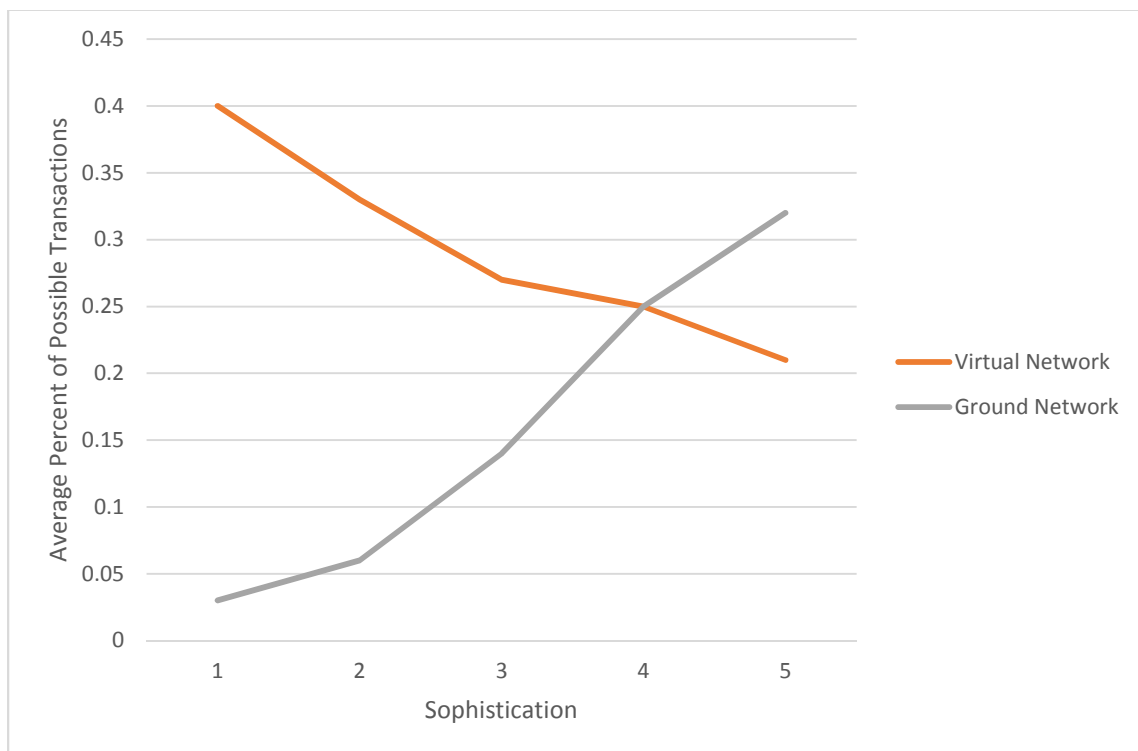


Figure 53 Average Percent of Possible Transactions in Virtual and Ground Models

5. Conclusion

Due to their high entry costs, low transaction cost environment, and relatively symmetric information, virtual black markets exhibit much less hierarchy but more monopolistic tendencies than ground black markets. We measure hierarchy using path length, degree, and betweenness and measure monopolistic tendencies using density and strong and weak clustering. We build upon Buchanan's (1973) and Shelling's (1971) work about the emergence of varying market structures. However, we find that different market network structures emerge with the same illicit goods, given different constraints. The concentration of the market in the Internet black market is higher than the ground market, suggesting that the extent of monopolistic tendencies are contributable to the structure of the market, not the good being exchanged.

This paper is a first attempt to disentangle the peculiar differences between digital drug marketplaces and ground markets, particularly with regards to network structure. This research serves to inform future study on digital market structure, and has numerous applications in other fields of research. The particular way in which this digital market shortens the distance between buyers and sellers is important to understanding the emergence of other digital markets. Because we find that virtual markets are less hierarchical and more monopolistic than ground markets, we build upon the contributions of Eilstrup-Sangiovanni and Jones (2008) and Arquilla and Ronfeldt (2001). We find that different market constraints, namely geographic limitations and the availability of reputation, are driving the extent to which a network is hierarchical and/or monopolistic.

Our results suggest future work particularly in the field of market monopolization, namely what market characteristics lead to more or less monopolization and when we can expect monopolistic markets to happen.

The less hierarchical nature of the virtual black markets suggest that they will be much more difficult to dismantle and disrupt. Standardized overarching improvements and changes will be more difficult in this type of network, however, because it is so diffuse, it will be more difficult than ground markets to target and take down. As the global economy shifts towards digital trade, how will participants adjust their behavior? How will policy makers and law enforcement adjust their behavior? Our analysis suggests that virtual markets result in a further shortening of the links between market participants and a further flattening of the market. This decentralized network structure suggests that it is quite robust.

Finally, this opens new avenues of analysis in law and economics with regards to the legalization of drugs. Legislation based on old models of the structure of modern drug markets will inevitably fail to meet their goals. They will bring in less tax revenue as user continue to use digital black markets, or even push more users into the digital black markets.

Appendix

Tables:

Table 4: Unedited List of Drug Types Parsed from Dark Web Data					
Weed	LSD	Oxycodone	Other	Steroids/PEDs	Methandroste- nolone
Cocaine	Dissociatives	Analgesics	Opium	FA's	Drostanolone
Heroin	MDMA	Drugs	Synthetic	Anabolic Steroids	Metabolism
Alcohol	Edibles	Concentrates	Methylphenidate	Hydromorphone	Oxymorphone
Stimulants	Opioids	Shrooms	DOx	FMA's	Dapoxetine
Ecstasy	DMT	Diazepam	Drug paraphernalia	Nootropics	Vardenafil
2C-Family	NBOMe	Benzos	Intoxicants	General health	
Human Growth Hormones	5-MeO-Family	Psychedelics	Relaxants	Prescription	
Alprazola m	4-HO-Family	GHB	Chemicals	Tadalafil	
Cannabis	Mescaline	Entheogens	Antidepressant	Forgeries	
Speed	4-ACO-Family	Sildenafil Citrate	Amphetamine	FMC's	

Figures:

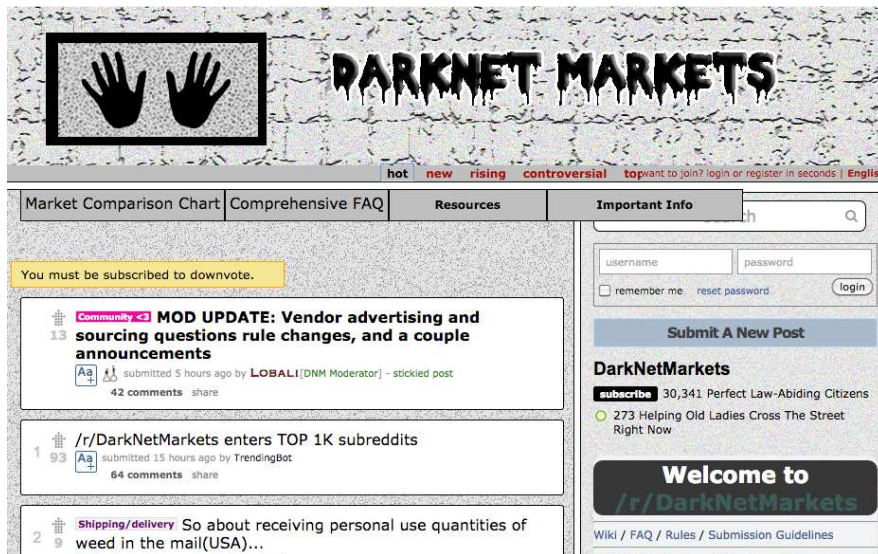


Figure 1 Darknet Markets 1

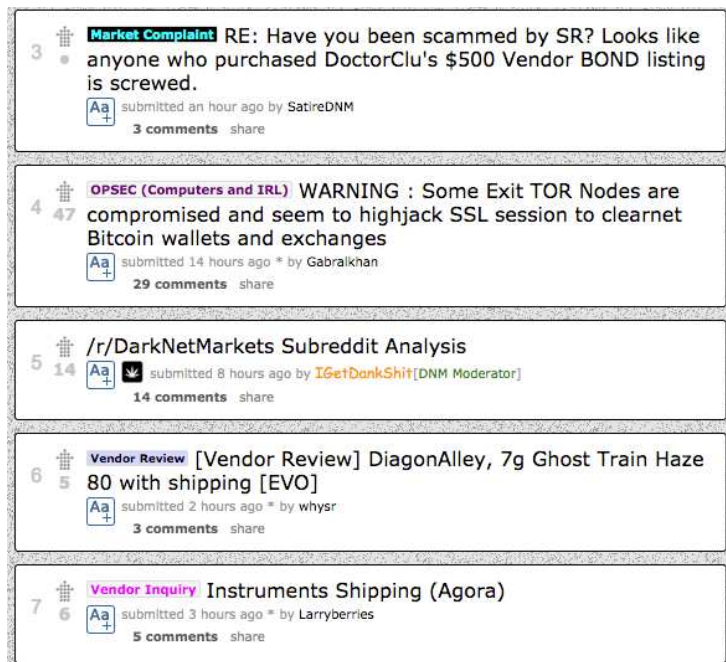


Figure 2 Darknet Markets 2

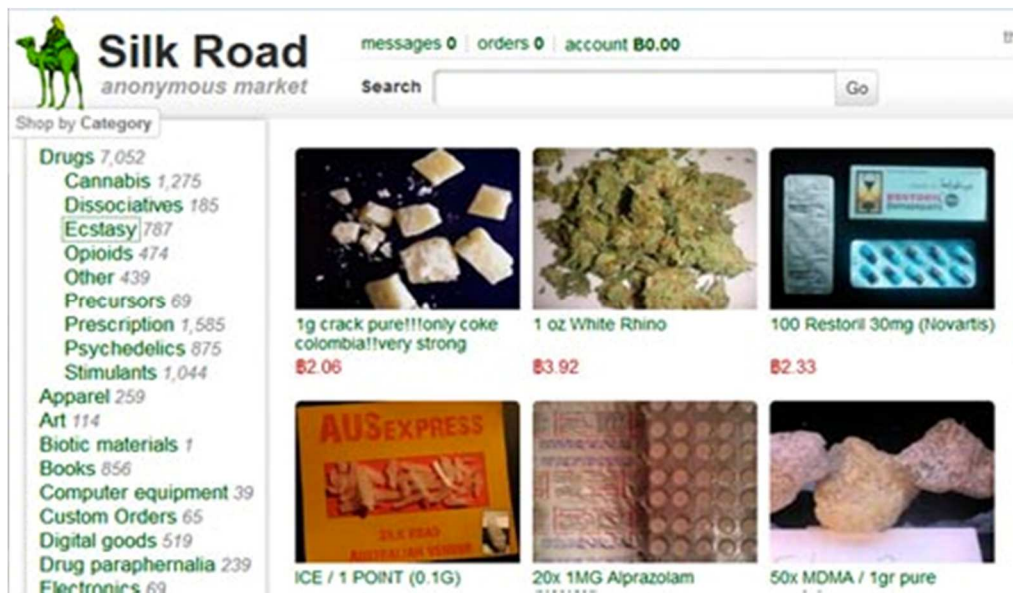


Figure 3 Silk Road 1



Figure 4 Silk Road 2

rating	feedback	freshness
★★★★★	Extremely good product for the price, I am a satisfied customer. Will call again.	1 day
★★★★★	awesome	1 day
★★★★★	Perfecrt	1 day
★★★★★	perfect as usual xxx	1 day
★★★★★	Fuck I was getting really worried! Delivery to Germany 13 days after marked shipped! I was starting to doubt anything in the world. Bit sticky but it will be excellent. Love you DM, sorry for the unnecessary message! efwnlirewtn435ds	1 day
★★★★★	always the same shit!!!! THE BEST SHIT YOU CAN GEET HERE :) 10/10	2 days
★★★★★	good communication with the vendor. not the same hight quality as othertimes but still good	2 days
★★★★★	Quick delivery, excellent stealth	2 days
★★★★★	Received the weed, great grass great stealth, recommended vendor.	2 days
★★★★★	8 Working days to UK - Great Product *****	2 days
★★★★★	5 Days to UK; Fantastic product for price, extrememly kiefy; 1g overweight, quite stalky; Reliable and speedy vendor! 5/5	2 days
★★★★★	My 2nd order, and as before im amazed with this guy :-> 7 days to UK and quality is top standard. I will be back very soon...	2 days
★★★★★	Good Delivery and good smoke	2 days

Figure 5 Feedback

shipping options

description	est. delivery	shipping price	
Free Shipping (non-tracked mail)	9 days	฿0.000000	add to cart

item feedback

30 day average: **4.90**
60 day average: **4.90**
Overall average: **4.89**

Figure 6 Item View



Figure 9 Darknet Market Lifespan

Support

Welcome to the support section. Here, you can open support tickets and view the status of your existing tickets. Please read the FAQs before requesting support. Old tickets will disappear 5 days after being closed. Click on the subject of the ticket to view the associated messages. A support ticket can have 3 states:

Processing: The ticket is waiting for a staff member to respond.

Answered: The ticket has been answered by a staff member, click the subject to view more.

Closed: The case is resolved and the support is finished. If you have a different issue, open a new ticket.

Support Tickets

ID	Status	Staff member	Subject	Last action
----	--------	--------------	---------	-------------

You currently have no support tickets.

[Request support](#)

Also take note of the PGP key below, it is the server's public key and is used for all official announcements.

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1

```
mQENBFU7NTEBCACvnZkiewS4OZM93+w1LYIz634I6b02Yvtqd+itGU5CbZ0uZGYJ
Pm6yDsEPtD+9tEz4ABSOQQuNI/SgzEbnh0sIH8nbpACzLPQpbnbH4U12btfTnGR
gQbEVBF0xqXk8OYeGwGd5UG3XOtKXZUe0rFh5JGMLjkab+38IMIn0ATuomxUgxi
s4EwN/tyIzREDtsJg6AWkOSNwgtHAtK95xYvA7mjTZxUQeXy+8l7NtGb5Ik7lZPG
VgwRCgLCY2UCLs8/jC3CNwFMe0Zm4ONprjeZf93F5KQflkalms4p7EbRgnOd019V
qmmSpgCTNpNkVjoWV4KhvEDLhmTa1YWY9A3NABEBAAG0HEFscGhhYmF5IDxBbHBBo
YWJheUBub25lLnNvbT6JATYEEwEKAFAIU7NTECGwMFCwkIBwMFFQoJCAAsEFglB
AAIeAQIXgAAKCRDgGaRP3Z3MZrK+B/9n5VvUEM3M13rZ1e5SUG3lobKY7denZUJc
0SYaZ4gQNoa0Erxfi8QZ7G11sXdQXsmhGzfXYHKwB94nbRp7X6e3VYub/7RZqn+Q
mwOkiumUmGwmFi8nFFVIDk3eQIHv/RdU6C6E8eRMzXGLhKspnVQ3tMQSFQ5YOWKq
IjhlBikV4GTc2B5W7r3J8TRdikVNvdPL37OTPg9nVPYwQVklM4TfxAdSJPkitmm
MNbfYA/br/JMH36VcoDfuhysaLW5V78tOCdG5ILGijvcCVUGCKEP5PcQs791+km
aRlgeMNLQRQEPbme3Cs99cFNOhPoq7vMciwZr3F+pVdAXt4xXqeHNuQENBFU7NTEB
CADqcKXZmU3sLctJoSfkvva1Ke90Tys6zAM0pJ2NQ48um974uFEmqkeZMbx2ix8W
rTukBAscHicu/6FvUWeS0jPYOA9bkHq9VjVZq0YukgwODFhFRWlQY2wIlx4nVHhs
```

Figure 10 Support (Support, 2017)

2Kg Critical Haze Indoor - TOP Quality Weed



฿10.04

€10600

Vendor

BHOLabs (90) (5.00) (👤 25, 5/5)

(📦 14, 5/5) (📅 8/0/0) (👤 50~70, 5.0/5)

Trusted vendor **Yes** (👍)


Ships to **Europe, United Kingdom**

Ships from **Spain**

Escrow **No**

[View offer](#)

Figure 11 Product on Dream Market (Shop: Dream Market, 2017)



10x ★ PINK RED BULL XTC PILLS ★ STRONG 270 MG MDMA ★ from The PartySquad NL

2017 PROMO DEAL: Did you order any of our products? Post a review thread and get 5 BLUE PUNISHER XTC PILLS FREE. Upload a detailed review to either AlphaBay Forum or Reddit's Darknet forums. Add at least one picture of the products and send us a PM on the market with a link to your review thread. Here's an example: (cleartnet link) https://www.reddit.com/r/DNMUK/comments/5cr96w/vendor_review_par...

Sold by **PartySquadNL** - 5298 sold since Jul 8, 2016 **Vendor Level 8** **Trust Level 7**

	Features		Features
Product class	Physical package	Origin country	Netherlands
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	FE Listing 90%

Bulk Discounts			
Bulk Discount	From qty 2 to 4	USD 21.90	0.0193 BTC
Bulk Discount	From qty 5 to 9	USD 19.90	0.0176 BTC

vacuum sealed + stealth (decoy) + PRIORITY shipping - 1 days - USD +4.75 / item

Purchase price: USD 23.90

Qty: **Buy Now** **Queue**

0.0211 BTC / 1.2238 XMR

Figure 12 Product on AlphaBay (Listing Options: AlphaBay Market, 2017)

Description	Bids	Feedback	Refund Policy
Listing Feedback			
Buyer	Date	Time	Comment
👤 a**2	April 5, 2017	01:40	2nd Order, FE because trustable and best quality
👤 s**3	April 3, 2017	18:18	slight delay in mail but all round perfect!
👤 t**o	March 31, 2017	05:18	ant come yet but got 100% faith n quilty speaks for self nice work
👤 m**4	March 29, 2017	23:39	6DD. Pleased with the speedy delivery, and the redbulls are always good 10/10
👤 V**2	March 28, 2017	15:46	wieder mal alles bestes besten teile die es gibt jetzt schon 5 mal bestellt und immer alles gelommen
👤 g**t	March 26, 2017	19:50	FE because vendor is very awesome -)
👤 3**s	March 26, 2017	15:24	Great gear, fast postage
👤 S**r	March 25, 2017	11:05	incredibly fast delivery
👤 t**v	March 24, 2017	23:59	perfect
👤 t**y	March 24, 2017	22:37	6DD to Spain - Perfect as always
👤 S**_	March 24, 2017	20:03	
👤 s**a	March 24, 2017	18:09	
👤 p**z	March 24, 2017	14:08	A+++! 6D to UK with Weekends! Everything OK! Will buy more in future!
👤 m**5	March 24, 2017	13:14	good good good thanks
👤 g**6	March 24, 2017	05:16	good clean no come down
👤 j**u	March 24, 2017	04:41	

Figure 13 Listing Feedback on AlphaBay (Listing Options: AlphaBay Market, 2017)

Feedback

Rating	Comment	Buyer	Date
★★★★★ (5)	alles super 10 Gram - Cocaine! VERY HIGH COCAINE CONTENT! 99,248%	M***1	03/29 04:23 pm

Figure 14 Listing Feedback on Wall St. Market (Featured Listings: Wall St. Market, 2017)

↑

3

↓

Dutchexpress banned

submitted 11 months ago by prevlaa

I see that this vendor was banned I'm concerned, reading his last feedback because I a month ago tried to make an order from him he told me "out of stock" and then he was very pushy, "I'll give you this for the same price, or this ..." I finally explained to him that I have no more BTC think I made a transaction with another vendor, then he left me alone but I'm thinking I sent him my personal data encrypted of course but still does anyone have to tell me something

Reply

Subscribe

Report

↑

HANSA Staff [222]

4 points

11 months ago (last edited: 11 months ago)

↓

As Pegasus said, he/she had a lot of unanswered 2-2 disputes and if we have to refund the first 2-2 dispute from our own funds we always ban the vendor. As you know 2-2 escrow cannot be accessed by 1 entity alone.
In 2-3 disputes the buyer can always withdraw himself but with 2-2 we have to ban the vendor to avoid further (monetary) damage.

Reply

Report

↑

Pegasus [394]

4 points

11 months ago

↓

He stopped replying to disputes, and did not ship out his product.

Reply

Report

↑

prevlaa [173]

[OP]

3 points

11 months ago

↓

thank you pegasus

Reply

Report

Figure 15 Forums Hansa 1 (Forums: Hansa, 2017)

↑

3

↓

Royaldrug Banned - Refund Possible?

submitted 7 months ago by Idavis300a

I'm going to guess the answer to this question is no but it's worth a shot. I had two tracked orders with Royaldrug that never showed any updates after clearing US customs 6 weeks ago. He refunded one of the two orders on the condition that I finalized the second order, so basically a 50% refund. Since it appears that he was scamming rather than having packages seized, is there a way to get that other order refunded? Or since I had finalized it (believing that it was a seizure rather than a scam), am I out of luck?

Reply

Subscribe

Report

↑

Orthorhombic [4]

2 points

7 months ago

↓

I've been in contact with him for literally months. This was last contact. I'm not worried at all. Read my post at the bottom of this thread also.

should be fine, but i would not response because i dont have access to my PC

available around 11 september*

Reply

Report

Figure 16 Forums Hansa 2 (Forums: Hansa, 2017)

125

Top Vendors

bestcoastbud	[+2315 -3]	★ Level 13
DutchMasters	[+195 0]	★ Level 13
dutchcandyshop	[+2127 -7]	★ Level 12
Karmaceuticals	[+2923 -1]	★ Level 12
Saint_Symbiosis	[+2291 -6]	★ Level 12
Mr_Taffy	[+1809 0]	★ Level 12
DrunkDragon	[+6194 -58]	★ Level 12
arctic	[+291 0]	★ Level 11
GoombaShop	[+216 -1]	★ Level 11
ProfessorDark	[+4555 -94]	★ Level 11
YOURDEALER	[+2107 0]	★ Level 11

Figure 17 Hansa Top Vendors (Welcome: Hansa, 2017)

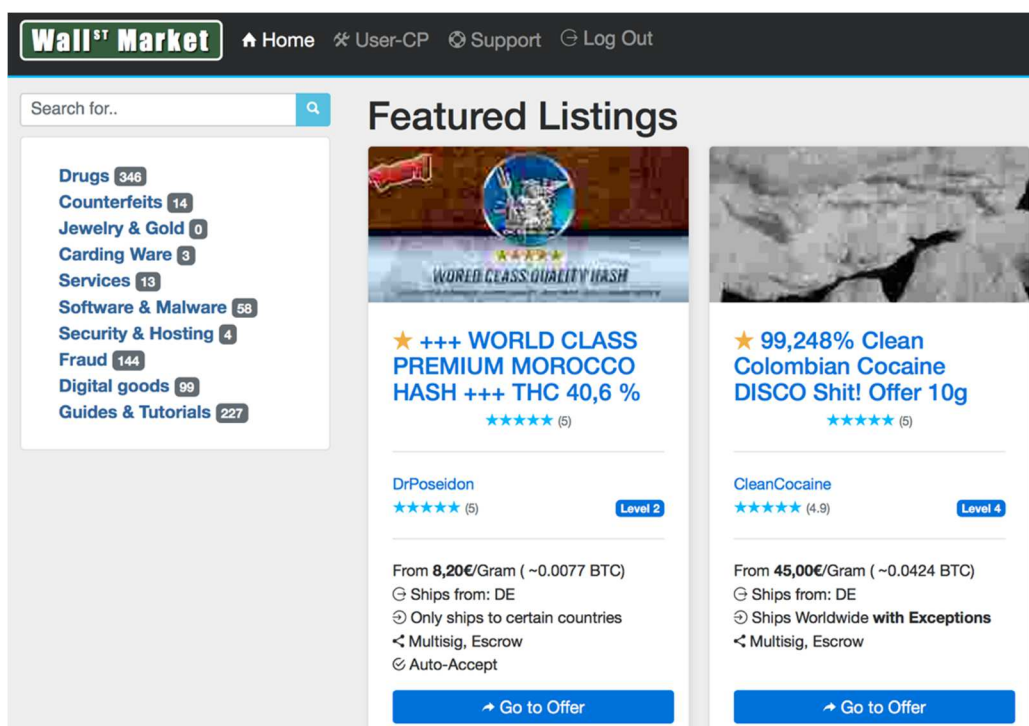


Figure 18 Wall St. Market Featured Listings (Featured Listings: Wall St. Market, 2017)

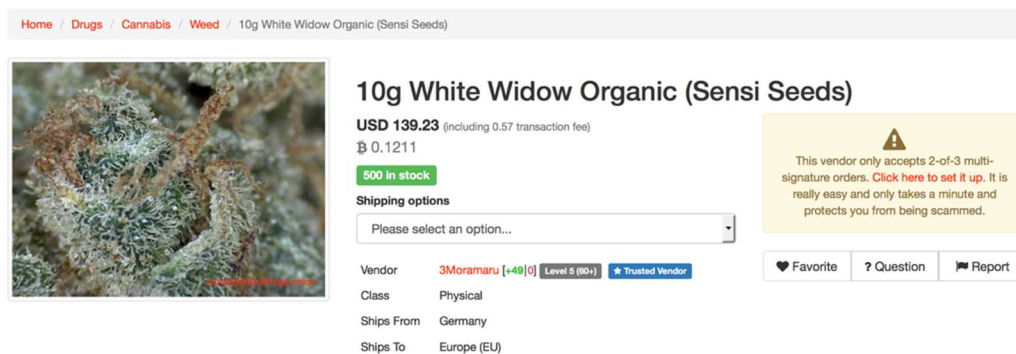


Figure 19 Hansa Drugs (Drugs: Hansa, 2017)

valhallaxmn3fydu.onion
All products
My purchases
Messages
Account (0.0 BTC)
Log out



You don't have enough funds for this product. Start by loading balance to **your account**.

20g Super Silver Haze Organic - top-end medical quality


264 EUR (0.246661 BTC)
more than 25 pcs in stock
3M/moramaru (2359 / -22)
Germany → Germany

Domestic (included)
1
Buy

- Name: Super Silver Haze Organic
- From: Holland
- Grade: A+++++
- Genetics: Skunk x Northern Lights x Haze.
- Effect: Great energetic body high

Super Silver Haze was the first prize winner at the High Times Cannabis Cup in 1997, 1998 and 1999 and also won awards at the High Times harvest festival. Helped Set the Standard for Genetic Excellence the Late 1990's. This sticky sativa will leave you with a great energetic body high. Genetics: Skunk x Northern Lights x Haze. Strong, fast-hitter, long lasting effect. Super Silver Haze Offers A Well Rounded Experience With Full Flavors.

Figure 20 All Products on Valhalla (All Products: Valhalla, 2017)



Favorite

★FREE SAMPLE★ COCAINE (PERU)AAA+++ uncut above 90% HIGH QUALITY Flakes Fishscale

Naturalminds [+29 | 0] ★ Level 4

Ships from: Germany


Also available:

★FREE SAMPLE★ COCAINE (PERU)AAA+++ uncut above 90% HIGH QUALITY Flakes Fishscale

USD 5.91
₿ 0.0052

Buy Now

Views: 4616



Favorite

2 XTC Pills 220mg (MDMA) 84% Ikea pencil FREE SAMPLE ONLY PAY SHIPMENT

DreamShop [+156 | 0] ★ Level 7 (200+)

Ships from: Netherlands

Also available:

2 XTC Pills 220mg (MDMA) 84% Simcards FREE SAMPLE ONLY PAY SHIPMENT	USD 1.57 ₿ 0.0014
5 XTC Pill 220mg (MDMA) 84% Purity ikea pencil	USD 15.57 ₿ 0.0138
5 XTC Pill 220mg (MDMA) 84% Purity Simcards	USD 15.57 ₿ 0.0138
10 XTC Pill 220mg (MDMA) 84% Purity Simcards	USD 28.57 ₿ 0.0253
10 XTC Pill 220mg (MDMA) 84% Purity Ikea pencil	USD 28.57 ₿ 0.0253
20 XTC Pill 220mg (MDMA) 84% Purity Ikea pencil	USD 55.57 ₿ 0.0492

(8 additional variants available)

USD 1.57
₿ 0.0014

Buy Now

Views: 361756

Figure 21 Free Sample Hansa (Drugs: Hansa, 2017)

Report | Quote

Dream Market
1chudifeyqm4ldjj.onion
jd6yhuwcivchvdt4.onion
t3e6ly3uoi14zcw2.onion
7ep7acr1kuzdcw3l.onion
 Established 2013

2017-03-07 04:56:46

ryder
 Member
 From: Weedopolis
 Registered: 2016-03-08
 Posts: 19

I ordered 4 ounces like 3 weeks ago and it turned up so idk wtf is going on with him seems so hit and miss. Ordered another 4 ounces in escrow though. No update as to whether he's sent it or not. Do you think I should just cancel while I still can?

 Smoke weed everyday

Report | Quote

#6

SpeedStepper
 Administrator


Have unlisted luciphero and disabled further vending . no further deal possible until issues are solved

Report | Quote

2017-03-07 15:20:09

WeedyDE2
 Member
 Registered: 2017-03-06
 Posts: 6

Many thanks! Got refund from diapute thanks Spannishconnect or other support. They lies again and said after refund it is shipt.....

 I only can say again DO NO FE!

 Regards and thanks Dream!

Report | Quote

Figure 22 Dream Market Forums 1 (Forums: Dream Market, 2017)

DreamMarket Forum

DreamMarket user forum.

[Index](#)
[Search](#)
[Profile](#)
[Logout](#)

Logged in as **VonMises764**
 Last visit: Today 18:58:10

Topics: [Posted](#) | [New](#)

[Index](#) » [Scams](#) » [banned kushtime](#)

Pages: **1**

Yesterday 06:22:40

#1


heinrich123
 Member
 Registered: Yesterday
 Posts: 1

vendor kushtime
 i have ordered one time with no problem.
 the second time i have ordered on 23th march and it were marked as sent on 25th march and i still got nothing...
 now i watch today and hes banned. dont tell me that i wont get my money back..

Report | Quote

Yesterday 08:29:49

#2

SmallWood
 Moderator


If you didn't F.E. your money will be refunded from escrow. Kushtime was banned today 04/04.

Report | Quote

Pages: **1**

Post reply

Figure 23 Dream Market Forums 2 (Forums: Dream Market, 2017)

129

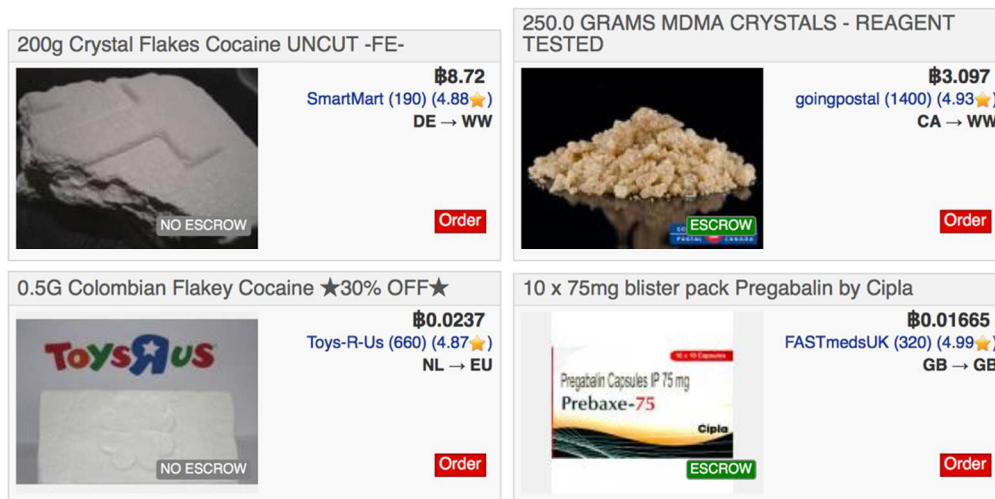


Figure 24 Shop Dream Market (Shop: Dream Market, 2017)

? How do I go about having feedback removed?

Feedback can be removed in the following cases:

- At the customers request
- Feedback with blackmail (provable beyond doubt)
- Feedback with private and critical information to the vendors operation.
- Partially refunded orders were a deal to not leave feedback or to remove feedback was made.
- Feedback containing extreme profanity or insults can temporarily be removed. The customer will be allowed to resubmit

We cannot remove feedback if:

- The customer is inactive or ignores your request to refund
- The proof of any of the above is encrypted and not verifiable to us.

Feedback removal cannot be enforced through your terms and conditions
Removal may only be requested once per feedback, our decision after review will be final.

For all requests please open a ticket under the "feedback removal request" category.

Figure 25 Remove Feedback (Knowledge Base and Support, 2017)

Hello,
is is a message that I would like to have encrypted. anks,
A user

Figure 26 PGP 1 (Mounteney et al., 2016, pg. 45)

-----BEGIN PGP MESSAGE-----

hQIMA3mulckJMVeCARAAoliWbrv6tYyXcA2tMs16Avp Ng37bt/eLsX3EdYS5YWMCl3Cictc8y93IMhOJNWRDL mt1Zrj9kDcE
ysCFePrRLUzxQQdFqsWh29VTa7vfKT pYCSXhsgUft0bPu62ISl+sYR51CWaE/bAtSwF7fqtKI4
AYUG3jeedHF8QScTtcCM15eNmp7TWZvURZT3kq6rW AVoSt938XN3JZhHd2SvX1qhOwqjoHGaQE+Kl2ejaZ8jr
u7Javwq3ix3/NF+b7EXBdM7eBb10Z1/sLEcgkyp1vEO8 RJ8HtXEfl g/TE+u+JH11IfcUxxafPZFNKp8AJhAvEe/r/
x5qABKEPBXYxDOxBT84i+aWgGSN5X1nx0Z2j8VyqWh xdmkugok/XNL0KbuH2sHIBAWsABYNTfbzm612WihhN
akEbyP5V719VvFBR1vr1bOP4RTj35xCi/V838V8cUku0 +U1YuWd+24avMHivRILodZqLhe5K9C/JyP22E/m4Ww
sa0ZPemm4g7vCKQWUDWRaa/OaBu4N1q37hVp83dj ED5dqSDmt15DU/ec65a7Mb3aKxajqQqwk7ivq0cBme
YfbWlekREZU2QTe6Vq6P5Tz94MfwJGNxOiDooEMGv 82AqPBjyY ArF50znAcqU9raqUMpH4EY1x+mUIJWir+a
6adimlEg1wXhje5LG0lc63SqwFxoXD8m+Swd02jbGLlI HaSnNJH0VQE15KS5JkbHm9M3qtd27vGxqKGlnnrWf
eeuc2ljsqmdtjwatCL7CQNRqSOC+g8OPowfd6unDF3 mIMOW9CjIGik89FTJPeyy6XCPd7vBezAstdplQ43W
THucHtly4ezScEy36hqKtSe28P40ZBVplw6MXH65ZG hLKl c4MlJTS3qXVrGZL4THn5dRF1osIjGMOELIA==

=iJXY

-----END PGP MESSAGE-----

Figure 27 PGP 2 (Mounteney et al., 2016, pg. 45)

sticked post **Forbidden goods on HANSA**
submitted 1 year ago by Pegasus

Any goods on the following list are forbidden and grounds for immediate ban without warning

- Anything in relation to "Teen leaks".
- Animal pornography
- Child pornography
- Toxins or Poisons
- Human trafficking
- Murder for hire
- Living animals
- Human organs
- Ammunition
- Explosives
- Snuff films
- Weapons
- Bombs

This includes related tools, videos, guides, tutorials, forum posts, mentions in your messages or vendor profiles.

Should you see such material please immediately report it to Support.

Figure 28 Forbidden Goods on Hansa (Forums: Hansa, 2017)

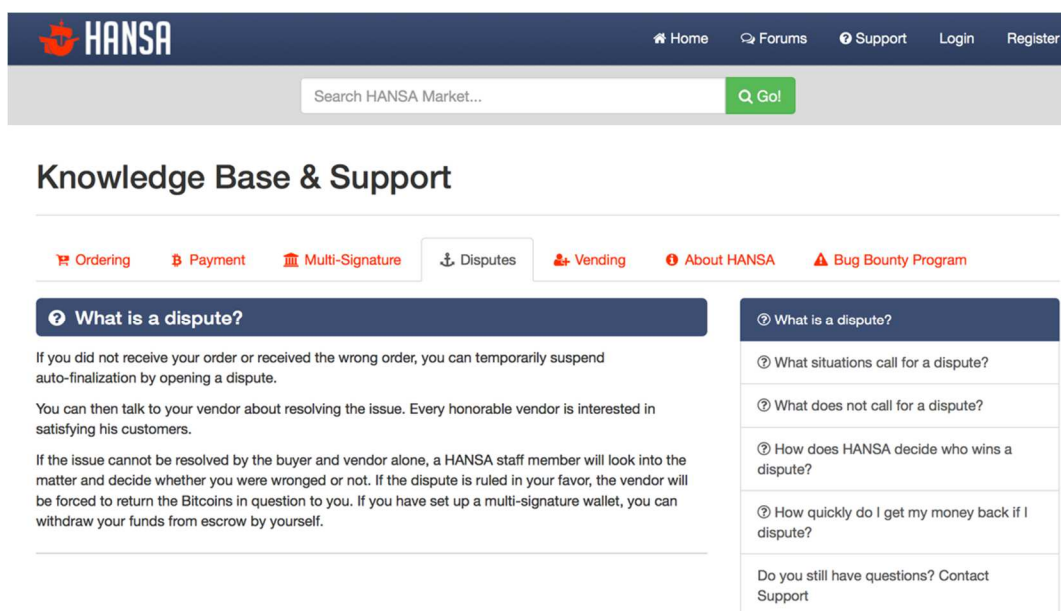


Figure 29 Hansa Knowledge Base and Support (Knowledge Base and Support: Disputes, 2017)



Figure 30 Vendors (Bakken, 2015)


```

to setup
  ifelse VirtualNetwork? = TRUE [
    ca
    reset-ticks
    create-turtles numAgents ;;this
    set numTransactions 0
    ask turtles [
      set reputation random-normal 4.82 0.63 ;;empirically derived from Deep Web data
      setup-agent-sophistication
    ]
  ]

```

Figure 31, To Setup

```

to decideToBuyMoreDrugsVirtual
  if ((stock / consumption) < tolerance) [
    set possible-sellers other turtles
    set myBuyingAmount (consumption * (random-normal 5 1))
    ask possible-sellers [
      let stockAfterSale (stock - myBuyingAmount)
      let stockConsumption (stockAfterSale / consumption)
      if stockConsumption > tolerance [set Dealer1? TRUE]
    ]
    set possible-sellers possible-sellers with [Dealer1? = TRUE]
  ]

```

Figure 32, Decide to Buy More Drugs Virtual 1

```

to decideToBuyMoreDrugsGround
  if ((stock / consumption) < tolerance) [
    set possible-sellers other turtles in-radius own-sophistication
    set myBuyingAmount (consumption * (random-normal 5 1))
    ask possible-sellers [
      let stockAfterSale (stock - myBuyingAmount)
      let stockConsumption (stockAfterSale / consumption)
      if stockConsumption > tolerance [set Dealer1? TRUE]
    ]
    set possible-sellers possible-sellers with [Dealer1? = TRUE]
  ]

```

Figure 33, Decide to Buy More Drugs Ground 1

```

turtles-own [
  reputation ;empirically dervied from deep web data
  own-sophistication ;normally distributed around the average sophistication specified in the model
  agents-in-radius ;unique to the ground model...the number of agents te each agents can see/reach
  possible-sellers ;an agentset that each agents creates and whittles down when decided who to engage in a transaction with
  imperfect-reputation ;unique to the ground network...it is the normally distrubuted around the agents true reputation
  comments ;empirically dervied from deep web data...used only in the virtual network
  stock ;the amount of drugs an agent has...normally distributed and based around the agent variable "own-sophistication"
  consumption ;the amount of drugs an agent consumes at one time...normally distributed around the around the average sophistication specified in the model
  tolerance ;the number of "doses" of a drug and agent wants to keep on hand
  Dealer1? ; a flag showing if an agents has enough drugs to be considered as a possible dealer
  highRiskSeller? ;a flag denoting whether or not a sellers reputation is above or below the risk threshold specified in the model - unique to virtual network
  Risk ;variable noting if the buyer is risk loving, risk averse, or risk neutral - unique to virtual network
]

```

Figure 34, Agents

```

to setup
  ifelse VirtualNetwork? = TRUE [
    ca
    reset-ticks
    create-turtles numAgents ;;this
    set numTransactions 0
    ask turtles [
      set reputation random-normal 4.82 0.63 ;;empirically derived from Deep Web data
      setup-agent-sophistication
      set comments random-normal 106 118 ;;empirically derived from Deep Web data
      setup-stock
      setup-consumption
      setxy random-xcor random-ycor
      set tolerance random-normal 5 2
      setRiskAversionAndReputation ;assign the distribution of buyers and whether they are risk averse/loving/neutral
    ]
  ]
end

```

Figure 35, To Setup 2

```

set sumStock (sum [stock] of turtles)
][
ca
reset-ticks
create-turtles numAgents ;;this
set numTransactions 0
ask turtles [
  set reputation random-normal 4.82 0.63 ;;empirically derived from Deep Web data
  setup-agent-sophistication
  set shape "person"
  setup-stock
  setup-consumption
  setxy random-xcor random-ycor
  set tolerance random-normal 5 2
]
set sumStock (sum [stock] of turtles)
if Showsophistication? = TRUE [display-sophistication]
]

end

```

Figure 36, Set up Agents

```

to decideToBuyMoreDrugsVirtual
  if ((stock / consumption) < tolerance) [
    set possible-sellers other turtles
    set myBuyingAmount (consumption * (random-normal 5 1))
    ask possible-sellers [
      let stockAfterSale (stock - myBuyingAmount)
      let stockConsumption (stockAfterSale / consumption)
      if stockConsumption > tolerance [set Dealer1? TRUE]
    ]
    set possible-sellers possible-sellers with [Dealer1? = TRUE]

    ifelse Risk < 0 [
      set possible-sellers possible-sellers with [(highRiskSeller? = FALSE)]
    ][ifelse Risk > 0 [set possible-sellers possible-sellers with [(highRiskSeller? = TRUE)]]][if Risk = 0 [set possible-sellers possible-sellers]]

    ifelse ((count possible-sellers) = 2)[set possible-sellers max-n-of 2 possible-sellers [comments]]
    [ifelse ((count possible-sellers) = 1)[set possible-sellers max-n-of 1 possible-sellers [comments]]
    [ifelse ((count possible-sellers) = 0)[]
    [set possible-sellers max-n-of 3 possible-sellers [comments]]
    ;set possible-sellers max-n-of 3 possible-sellers [comments]

    set FinalDealer max-one-of other possible-sellers [reputation]
  ]
]
end

```

Figure 37, Decide to Buy More Drugs Virtual 2

```

to decideToBuyMoreDrugsGround
  if ((stock / consumption) < tolerance) [
    set possible-sellers other turtles in-radius own-sophistication
    set myBuyingAmount (consumption * (random-normal 5 1))
    ask possible-sellers [
      let stockAfterSale (stock - myBuyingAmount)
      let stockConsumption (stockAfterSale / consumption)
      if stockConsumption > tolerance [set Dealer1? TRUE]
    ]
    set possible-sellers possible-sellers with [Dealer1? = TRUE]

    ask possible-sellers [
      set imperfect-reputation random-normal reputation 2
    ]
    set FinalDealer max-one-of other possible-sellers [imperfect-reputation]
  ]
end

```

Figure 38, Decide to Buy More Drugs Ground 2

References

- (2015). *Black Market Risks*. <http://www.gwern.net/Black-market%20survival>.
- 30,000 anonymous services make up Tor's Dark Net. (2015, February 16). Retrieved January 25, 2017, from <http://www.dailydot.com/layer8/tor-dark-net-study-size/>.
- Acquisti, A., Dingledine, R. and Syverson, P. (2003), "On the economics of anonymity", *7th International Conference on Financial Cryptography*, Guadeloupe, 27-30 January, pp. 84-102.
- Afilipoaie, Alois and Patrick Shortis. (2015). The Growing Industry of Darknet Marketing. *GDPO Situation Analysis, Swansea University*. 1-4. <http://www.swansea.ac.uk/media/GDPO%20SA%20Marketing.pdf>.
- Akerlof, G. and J. Yellen. (1994). Gang Behavior, Law Enforcement, and Community Values. *Brookings Institution, Values and Public Policy*: Washington, DC.
- Allen, D. W. (1999). Transaction costs. *Encyclopedia of law and economics*.
- All Products: Valhalla. (2017). Valhalla. <http://valhallaxmn3fydu.onion/products/50227>.
- Alqahtani, Fahad A. (2014). A Fair Exchange & Customer Anonymity Protocol Using A Trusted Third Party for Electronic Commerce Transactions & Payments. *International Journal of Network Security & Its Applications*, 6(1), pp.59-7.
- Arquilla, J. and D. Ronfeldt. (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, CA: RAND Corporation, http://www.rand.org/pubs/monograph_reports/MR1382.html.
- Ashley Madison. (2017). Retrieved March 3, 2017, from <https://www.ashleymadison.com>.
- Axtell, R. (2000). Why Agents? On the Varied Motivations for Agent Computing in the Social Sciences. Working Paper. *The Brookings Institution*. pg. 1-12.
- Backhaus, J. (1979). Defending Organized Crime? A Note. *The Journal of Legal Studies*, 8(3), 623–631. Retrieved from <http://www.jstor.org/stable/724172>.

Bakken, S. A. (2015). Silk Road 2.0-A Study of Cryptomarkets in a Deleuze-Guattarian Perspective.

Baran,P. (1964). On distributed communications: IX security secrecy and tamper-free considerations. Memo RM-3765-PR,Rand Corp., Santa Monica,CA.

Barreto, Manuela and Naomi Ellmers (2002). The impact of anonymity and group identification on progroup behavior in computer-mediated groups. *Small Group Research*, 33(5), pp. 590-610.

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, 76(2):169-217.

Benson, B. L. (1989). "The spontaneous evolution of commercial law." *Southern Economic Journal*, 55(3), 644-661. Retrieved from <http://search.proquest.com/docview/56371368?accountid=14541>.

Black Market Risks. (2015). <http://www.gwern.net/Black-market%20survival>.

Brands, S. (2000). Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press: Cambridge, MA.

Briere, M., K. Oosterlinck, and A. Szafarz. (2013). *Virtual currency, tangible return: Portfolio diversification with bitcoins* ULB -- Universite Libre de Bruxelles, Working Papers CEB: 13-031. Retrieved from <http://search.proquest.com/docview/1438547719?accountid=14541>.

Broekel, T., P. Balland, M. Burger, and F. van Oort. (2014). Modeling Knowledge Networks in Economic Geography: A Discussion of Four Methods. *Annals Of Regional Science*, 53(2), 423-452. doi:<http://dx.doi.org.mutex.gmu.edu/10.1007/s00168-014-0616-2>.

Buchanan, J. M. (1973). A Defense of Organized Crime? *Economics of Crime and Punishment*. 119.

Buxton, J., and T. Bingham. (2015). The rise and challenge of dark net drug markets. *Policy Brief*, 7.

Chandler, Nathan. (2013, December 23). "How the Deep Web Works." Retrieved July 16, 2014, from HowStuffWorks.com website: <http://computer.howstuffworks.com/internet/basics/how-the-deep-web-works1.htm>.

Christin, N. (2012). "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," *Cornell University Library Working Paper*, 12-018.

Chang, J.-J., H. C. Lu, and M. Chen. (2005). Organized crime or individual crime? endogenous size of a criminal organization and the optimal law enforcement. *Economic Inquiry*, 43(3):661-675.

Chaum, D. (1981). Untraceable electronic mail, return addresses and digital pseudonyms. *Communications of the A.C.M.*, 24(2):84-88.

Chaum, D. (1998). The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(1):65-75.

Chen, A. (2011). The Underground Website Where You Can Buy Any Drug Imaginable. Retrieved April 4, 2017, from <http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160>.

Christin, N. (2012), "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," *Cornell University Library Working Paper*, 12-018.

Clay, Karen (1997). "Trade without Law: Private –Order Institutions in Mexican California." *Journal of Law, Economics, and Organization*, 13(1), 202-231.

Comparing Networks. (2008). Comparing Networks. In *Exploring Animal Social Networks* (pp. 141-162). Princeton University Press. Retrieved from <http://www.jstor.org/stable/j.ctt7sfqv.10>.

Dana, L. P. (2001). Introduction: Networks, Internationalization & Policy. *Small Business Economics*, 16(2), 57-62. Retrieved from <http://www.jstor.org/stable/40229137>.

DarkNet Markets. Retrieved October 14, 2014, from Reddit website: <http://www.reddit.com/r/DarkNetMarkets>.

Darknet Market. (2017). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Darknet_market&oldid=771022190.

DeepDotWeb: Surfacing The News From The Deep Web. (2017). Retrieved January 26, 2017, from <https://www.deepdotweb.com/>.

Deep Web: A Primer. (n.d.). Retrieved from <http://www.brightplanet.com/deep-web-university-2/deep-web-a-primer/>.

Dick, A. R. (1995). When does organized crime pay? A transaction cost analysis,

International Review of Law and Economics 5: 25-45.

Dingledine, Roger and Paul Syverson (Eds.). (2002). *Privacy Enhancing Technologies*. Springer-Verlag Berlin Heidelberg: PET 2002, LNCS 2482.

Dingledine, R., Mathewson, N., & Syverson, P. (2003, June). Reputation in p2p anonymity systems. In *Workshop on economics of peer-to-peer systems*(Vol. 92).

Dingledine, Roger, Nick Mathewson, and Paul Syverson. (2004). "Tor: The Second-Generation Onion Router." National Research Laboratory. Release Number 03-1221. 1-2602.

Dingledine, R. and S. J. Murdoch. (2009). Performance Improvements on TOR or Why Tor is Slow and What We're Going to do About it. *The Tor Project*.
<https://svn.torproject.org/svn/projects/roadmaps/2009-03-11-performance.pdf>.

Dolliver, D. S. and J. L. Kenney (2016). Characteristics of Drug Vendors on the Tor Network: A Cryptomarket Comparison, *Victims & Offenders*, 11:4, 600-620.

Dornbach P., Németh Z. (2003) Privacy Enhancing Profile Disclosure. In: Dingledine R., Syverson P. (eds) *Privacy Enhancing Technologies*. PET 2002. Lecture Notes in Computer Science, vol 2482. Springer, Berlin, Heidelberg.

Downey, A. B. (2012). *Think Java: How to Think Like a Computer Scientist*. Green Tea Press. <http://www.greenteapress.com/thinkapjava/thinkapjava.pdf>.

Drugs: Hansa. (2017). Hansa. <http://hansamkt2rr6nfg3.onion/listing/23500/>.

European Central Bank (ECB) (2012), Virtual Currency Schemes, <http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf>. Featured Listings: Wall St. Market. (2017). Wall St. Market. <http://wallstyizjhkrvmj.onion/index>.

Fee for Becoming a Vendor/Seller on AlphaBay • r/DarkNetMarkets. (2016). Retrieved November 14, 2016, from https://www.reddit.com/r/DarkNetMarkets/comments/4ftrll/fee_for_becoming_a_vendorseller_on_alphabay/.

Fiorentini, G. and S. Peltzman. (1995). Introduction in *The Economics of Organised Crime* edited by G Fiorentini and S Peltzman, Cambridge University Press and CEPR.

Forums: Dream Market. (2017). Dream Market. <http://tmskhzavkydupbr.onion/viewtopic.php?id=26694>.

Forums: Hansa. (2017). Hansa. <http://hansamkt2rr6nfg3.onion/thread/913/>.

Friedman, Milton. Interview. *PBS: Commanding Heights*. N.p., 1 Oct. 2000. Web. 2 Mar. 2015.

http://www.pbs.org/wgbh/commandingheights/shared/minitext/int_miltnfriedman.html#1

Fries, A., Anthony, R. W., Cseko Jr, A., Gaither, C. C., & Schulman, E. (2008). *The price and purity of illicit drugs: 1981-2007* (No. IDA-P-4369). INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA.

Gallup. (2014). Investors Risk-Averse When It Comes to Retirement Savings, March 14, 2014. <http://www.gallup.com/poll/168197/investors-risk-averse-comes-retirement-savings.aspx>.

Gambetta, D. (1996). *The Sicilian Mafia: the business of private protection*. Harvard University Press.

Gambetta, Diego (2010). "Codes of the Underworld: How Criminals Communicate," Princeton, NJ: Princeton University Press.

Garoupa, N. (2000). The economics of organized crime and optimal law enforcement. *Economic Inquiry*, 38(2): 278-288.

Gaup, M. and M. Elizabeth. (2008). Quantification of Anonymity for Mobile Ad Hoc Networks. *Electronic Notes in Theoretical Computer Science*. 1-12.
www.elsevier.nl/locate/entcs.

Gehl, R. (2011). Ladders, samurai, and blue collars: Personal branding in Web 2.0. *First Monday*, 16(9). doi:10.5210/fm.v16i9.3579.

Greenberg, A. (2015). "Ahead of Sentencing, Ulbricht Defense Argues Silk Road Made Drug Use Safer." *Wired*, <https://www.wired.com/2015/05/ahead-sentencing-ulbricht-defense-argues-silk-road-made-drug-use-safer/>.

Greif, A. (1993). Contract enforceability and the economic institutions in early trade: The Maghribi traders' coalition. *American Economic Review*, 83: 525–548.

Greif, Avner (2012), "The Maghribi Traders: A Reappraisal?" *Economic History Review*, 65(2), 445-469.

Greif, Avner (2010), "Contract Enforceability and Economic Institutions in Early Trade: The Maghribi Traders' Coalition." *The New Institutional Economics of Markets*, Collective Volume Article, 432-455.

Greif, Avner (1989), "Reputation and Coalitions in Medieval Trade: Evidence on the Maghribi Traders." *The Journal of Economic History*, 49(4), 857-882.

Grinberg, R. (2011). "Bitcoin: An Innovative Alternative Digital Currency." *Hastings Science & Technology Law Journal*, 4, 160-207.

Good Wagon Books, University, P. S., University, P. S., & Website, C. (2017). Ross Ulbricht | LinkedIn. Retrieved February 6, 2017, from https://www.linkedin.com/in/rossulbricht?trk=public_profile_card_url.

Gunaratna, R. (2006). The Terror Market: Networks and Enforcement in the West. *Harvard International Review*, 27(4), 66-69.

Eilstrup-Sangiovanni, M. and C. Jones. (2008). Assessing the Dangers of Illicit Networks: Why Al-Qaida May Be Less Threatening than Many Think. *International Security*, 33(2), 7-44. Retrieved from <http://www.jstor.org/stable/40207130>.

Epstein, J. M. and R. Axtell. (1996). *Growing Artificial Societies: Social Science From the Bottom Up*. Washington, D.C.: The Brookings Institution.

Everton, S. F. (2012). *Disrupting Dark Networks*. New York, New York: Cambridge University Press.

Hardy, R.A. and J. R. Norgaard. (2015). Reputation in the Internet black market: an empirical and theoretical analysis of the Dark Web. *Journal of Institutional Economics*, 2015, pp 1-25. DOI 10.1017/S1744137415000454.

Holderness, C. G. and J. Pontiff. (2012). Hierarchies and the Survival of POWs during WWII. Forthcoming in *Management Science*.

Houser, D., & Wooders, J. (2006). "Reputation in Auctions: Theory, and Evidence from eBay." *Journal of Economics & Management Strategy*, 15, 353-369.

Hume, Tim. (Oct 5, 2013). *How FBI caught Ross Ulbricht, alleged creator of criminal marketplace Silk Road*. CNN. <http://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/>.

Hu, Xiaorui, Zhangxi Lin, Andrew B. Whinston, Han Zhang, (2004) Hope or Hype: On the Viability of Escrow Services as Trusted Third Parties in Online Auction Environments. *Information Systems Research* 15(3):236-249. <http://dx.doi.org/10.1287/isre.1040.0027>.

I am a Tor and Cybercrime researcher, AMA. (2015). Reddit.com/deepweb. https://www.reddit.com/r/deepweb/comments/3mqkxz/i_am_a_tor_and_cybercrime_researcher_ama/.

Internet Freedom in a Surveillance Society. (2015). Internet Freedom in a Surveillance Society. In *The Real Cyber War: The Political Economy of Internet Freedom* (pp. 180–202). University of Illinois Press. Retrieved from <http://www.jstor.org/stable/10.5406/j.ctt130jtjf.12>.

Introduction. (2017). Dream Market. <http://lchudifyeqm4ldjj.onion/help>.

Jankowski, M. S. (1991). *Islands in the Street: Gangs and American Urban Society*. Berkeley: University of California Press.

Jennings, W. P. (1984). A note on the economics of organized crime. *Eastern Economic Journal*, 10(3): 315-321.

Johnson, A., P. Syverson, R. Dingledine, and N. Mathewson. (2011). Trust-based Anonymous Communication: Adversary Models and Routing Algorithms. Creative Commons Attribution 3.0 License. 1-12. <http://freehaven.net/~arma/anonymity-trust-ccs2011.pdf>.

Jones, N. P. (2016). The State Reaction and Illicit-Network Resilience. In *Mexico's Illicit Drug Networks and the State Reaction* (pp. 19-46). Washington, DC: Georgetown University Press. Retrieved from <http://www.jstor.org/stable/j.ctt1c2crb0.7>.

Karjoth, Günter, Matthias Schunter, and Michael Waidner. (2002). Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data. 2nd Workshop on Privacy Enhancing Technologies, Springer Verlag. http://www.semper.org/sirene/publ/KaSW1_02.EP3P4PET.pdf.

Kesdogan, D, J. Egner, and R. Buschkes. (1998). Stop-and-go-MIXes providing probabilistic anonymity in an open system. In Proceedings of the *International Information Hiding Workshop*, LNCS 1525.

Kilmer, Beau, and Rosalie Liccardo Pacula. "Estimating the size of the global drug market: A demand-side approach." *A Report on Global Illicit Drug Markets 1998-2007* 25 (2009).

Klein, B., & Leffler, K. (1981). "The Role of Market Forces in Assuring Contractual Performance." *Journal of Political Economy*, 89(4), 615-641.

Knowledge Base and Support: Disputes. (2017). Hansa. <http://hansamkt2rr6nfg3.onion/support/9/>.

Kruithof, K., J. Aldridge, D. D. Héту, M. Sim, E. Dujso, and S. Hoorens. (2016). Internet-facilitated drugs trade [Product Page]. Retrieved March 9, 2017, from http://www.rand.org/pubs/research_reports/RR1607.html.

Lazear, E. and S. Rosen. (1981). Rank Order Tournaments as Optimum Labor Contracts. *Journal of Political Economy*. 89: 841-864.

Leeson, Peter T. (2005a). "Endogenizing Fractionalization." *Journal of Institutional Economics*, 1(1), 75-98. Retrieved from <http://search.proquest.com/docview/213620017?accountid=14541>.

Leeson, Peter T. (2005b). Self-enforcing arrangements in African political economy. *Journal of economic behavior & organization*, 57 (2), p. 241 – 244.

Leeson, P. T. (2007). An-arrgh-chy: The law and economics of pirate organization. *Journal of political economy*, 115(6): 1049-1094.

Leeson, P. T. (2009). The calculus of piratical consent: the myth of the myth of social contract. *Public Choice*, 139(3-4): 443-459.

Leeson, Peter T. (2010a). "Anarchy Unbound: How Much Order Can Spontaneous Order Create?," Cheltenham, U.K. and Northampton, Mass.: Elgar.

Leeson, P. T. (2010b). Pirational choice: the economics of infamous pirate practices. *Journal of Economic Behavior & Organization*, 76(3): 497-510.

Leeson, P. T. and Rogers, D. (2012). Organizing Crime. *Supreme Court Economic Review*, 20: 89-123.

Levitt, S. D. and S. A. Venkatesh. (2000). An Economic Analysis of a Drug-Selling Gang's Finances. *The Quarterly Journal of Economics*, 115(3), 755–789. Retrieved from <http://www.jstor.org/stable/2586895>.

Leyden, John. (Sept 11, 2015). "Walter Mitty" IT manager admits to buying gun on Dark Web: Cops chalk one up to undercover sting operation. The Register. http://m.theregister.co.uk/2015/09/11/dark_web_gun_purchase_bust/.

Listing Options: AlphaBay Market. (2017). AlphaBay Market. <http://pwoah7foa6au2pul.onion/listing.php?id=180000>.

Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., & Hubaux, J.-P. (2013). Game Theory Meets Network Security and Privacy. *ACM Comput. Surv.*, 45(3), 25:1–25:39. <https://doi.org/10.1145/2480741.2480742>.

Martin, J. (2014). *Drugs on the Dark Net: How Cryptomarkets and Transforming the Global Trade in Illicit Drug*. Palgrave Macmillan.

Mayntz, R. (2004). *Organizational forms of terrorism: hierarchy, network, or a type sui generis?* (No. 04/4). MPIfG Discussion Paper.

McCoy, D., K. Bauer, D. Grunwald, T. Kohno, and D. Sicker. (2008). Shining Light in Dark Places: Understanding the Tor Network. In N. Borisov & I. Goldberg (Eds.), *Privacy Enhancing Technologies* (Vol. 5134, pp. 63–76). Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved from http://link.springer.com/10.1007/978-3-540-70630-4_5.

McDonald, C., & Slawson, V. (2002). "Reputation In An Internet Auction Market." *Economic Inquiry*, 40(4), 633-650.

Melnik, M., & Alm, J. (2002). "Does a Seller's E-Commerce Reputation Matter? Evidence from eBay Auctions." *Journal of Industrial Economics*, 50(3), 337- 349.

Milgrom, Paul R., North, Douglass C. & Weingast, Barry R. (2010). "The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges and the Champagne Fairs." *The New Institutional Economics of Markets*, Collective Volume Article, 581-603.

Morgan, JP. "2012 Online Fraud Report." 2012. Accessed June 25, 2015.
https://www.jpmorgan.com/cm/BlobServer/13th_Annual_2012_Online_Fraud_Report.pdf?blobkey=id&blobwhere=1320571432216&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs.

Mounteney, J., A. Bo, and A. Oteo. (2016). *The internet and drug markets*. Luxembourg: Publications Office of the European Union.

Mueller, Dennis C. (1988). "Anarchy, the Market, and the State," *Southern Economic Journal*, 54,(4), 821-830.

Ogus, A. (2002). The Economic Basis of Legal Culture: Networks and Monopolization. *Oxford Journal of Legal Studies*, 22(3), 419-434. Retrieved from <http://www.jstor.org/stable/3600653>.

Onion Routing (2014). Retrieved September 7, 2014 from Onion Routing website: <http://www.onion-router.net/>.

Pfitzmann, A and M. Kohntopp. (2000). Anonymity, unobservability and pseudonymity — a proposal for terminology. In Designing Privacy Enhancing Technologies. Proceedings of the *International Workshop on the Design Issues in Anonymity and Observability*, LNCS 2009.

Piano, E. E. (2017). Free riders: the economics and organization of outlaw motorcycle gangs. *Public Choice*. 170: 1-19.

Posner, Richard A. (1980). "A Theory of Primitive Society, with Special Reference to Law." *The Journal of Law and Economics*. 23(1), 1-53.

Powell, Benjamin & Edward P. Stringham. (2009). "Public Choice and the Economic Analysis of Anarchy: A Survey." *Public Choice*, 140(3/4), 503-538.

Programming Guide. (2017). NetLogo 6.0.1 User Manual. <https://ccl.northwestern.edu/netlogo/docs/programming.html>.

Railsback, S. F. and V. Grimm. (2012). *Agent-Based and Individual-Based Modeling: A Practical Introduction*. Princeton, New Jersey: Princeton University Press.

Resnick, P. and R. Zeckhauser, 2001, "Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System," Mimeo.

Rouse, M. (2013). What is digital certificate? - Definition from WhatIs.com. Retrieved December 14, 2016, from <http://searchsecurity.techtarget.com/definition/digital-certificate>.

Sassenberg, K., and T. Postmes. (2002). Cognitive and strategic processes in small groups: Effects of anonymity of the self and anonymity of the group on social influence. *British Journal of Social Psychology*, 41(3), 463.

Schelling, T. C. (1971). What Is the Business of Organized Crime? *The American Scholar*, 40(4), 643–652. Retrieved from <http://www.jstor.org/stable/41209902>.

Scott, S. and M. Koehler. (2011). A Field Guide to Net Logo. George Mason University, Department of Computational Social Science, Version 1.1.

Shapiro, C. (1983). Premiums for High Quality Products as Returns to Reputations. *The Quarterly Journal of Economics*, 98, 659-680.

Shop: Dream Market. (2017). Dream Market. <http://lchudifyeqm4ldjj.onion/>.

Silk Road: Anonymous Market. (2014). silkroad6ownowfk.onion.

Skarbek, D. (2010). Putting the "con" into constitutions: the economics of prison gangs.

Journal of Law, Economics, and organization, 26(2):183-211.37.

Skarbek, D. (2011). Governance and prison gangs. *American Political Science Review*, 105(4):702-716.

Skarbek, D. (2012). Prison gangs, norms, and organizations. *Journal of Economic Behavior & Organization*, 82(1):96-109.

Skarbek, Emily Schaeffer (2008). "Remittances and Reputations in Hawala Money-Transfer Systems: Self-Enforcing Exchange on an International Scale." *Journal of Private Enterprise*, 24(1), 95-117.

Spergel, I. (1995). *The Youth Gang Problem: A Community Approach*. Oxford University Press: New York.

Stringham, Edward Peter. (2002). The Emergence of the London Stock Exchange as a Self-Policing Club. *Journal of Private Enterprise*, 17(2): 1-19.

Stringham, Edward. (2015). *Private Governance: Creating Order in Economic and Social Life*. New York and Oxford: Oxford University Press.

Support. (2017). AlphaBay Market. <http://pwoah7foa6au2pul.onion/contact.php>

Support: New Ticket. (2017). Wall St. Market. <http://wallstyizjhkrvmj.onion/support>.

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K. (2015). The challenges of personal data markets and privacy. *Electronic Markets*, 25(2), 161-167.
doi:<http://dx.doi.org/mutex.gmu.edu/10.1007/s12525-015-0191-0>.

Syverson, P. (2013). Practical Vulnerabilities of the Tor Anonymity Network. In D. F. Hsu & D. Marinucci (Eds.), *Advances in Cyber Security: Technology, Operations, and Experiences* (pp. 60–73). Fordham University. Retrieved from <http://www.jstor.org/stable/j.ctt13x07xx.7>.

Tapscott, Don and Alex Tapscott. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. New York, New York: Penguin Random House.

Taylor, Harriet. (May 19, 2016). Hit men, drugs and malicious teens: the darknet is going mainstream. Retrieved January 21, 2017, from <http://www.cnbc.com/2016/05/18/hit-men-drugs-and-malicious-teens-the-darknet-is-going-mainstream.html>

Tor Metrics. (2015). <https://metrics.torproject.org/about.html#client>.

Tor Project. (2015). <https://www.torproject.org/about/overview>.

Trautman, L. J. (2014). Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox?. *Richmond Journal of Law and Technology*, 20(4).

Tucker, Jeffrey (personal interview, September 23, 2014).

U.S. vs. Ross Ulbricht, Government Exhibit 940D. 14 Cr. 68. New York Southern District Court. 30 Sept. 2013.

Van Hout, M.C. and T. Bingham. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy*, Volume 25, Issue 2, March 2014, Pages 183–189.

<http://www.sciencedirect.com/mutex.gmu.edu/science/article/pii/S0955395913001722>.

Varese, F. (2001). *The Russian Mafia: private protection in a new market economy*. OUP Oxford.

Vendor CandyNL threatening to dox me and 200 others... Help! • r/DarkNetMarkets. (2017). Retrieved March 2, 2017, from https://www.reddit.com/r/DarkNetMarkets/comments/5irmal/vendor_candy_nl_threatening_to_dox_me_and_200/.

Weiser, Benjamin. (May 29, 2015a). *Ross Ulbricht, Creator of Silk Road Website, Is Sentenced to Life in Prison*. The New York Times. <https://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentenced-to-life-in-prison.html>.

Weiser, Benjamin (May 18, 2015b). *Silk Road, Online Black Market, Reduced Users' Risks, Defense Says*.

Welcome: Hansa. (2017). Hansa. <http://hansamkt2rr6nfg3.onion/>.

Wilson, J. L., T. E. Griffin, and L. M. Jessup. (2010). GSS Anonymity effects on small group behavior. *Academy of Information and Management Sciences Journal*, 13(2), 41-57.

WSM Forum. (2017). Wall St. Market. <http://x7bwsmcore5fmx56.onion/>.

Zerbe, R., Anderson, L., 2001. Culture and fairness in the development of institutions in the California gold fields. *Journal of Economic History* 10, 114–143.

Zimmermann, P. (1999). 'Why I wrote PGP', <https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html>.

Biography

Julia R. Norgaard received her Bachelor of Arts in Economics from the University of San Diego in 2012. She went on to receive her Master of Arts in Economics at George Mason University in 2015, concentrating on Public Choice, Applied Microeconomics, and Development. After finishing her Doctor of Philosophy in Economics at George Mason University in 2017, she began a position as an Assistant Professor of Economics at Pepperdine University in Malibu, California.