American Behavioral Scientist
1–24

DOI: 10.1177/0002764217734269
journals.sagepub.com/home/abs


Flow My FE the Vendor Said: Exploring Violent and Fraudulent Resource Exchanges on Cryptomarkets for Illicit Drugs

Kim Moeller[1], Rasmus Munksgaard[2], and Jakob Demant[3]

Abstract

A growing share of illicit drug distribution takes place using cryptomarkets that use encryption and anonymization technologies. The risks of law enforcement intervention and violence are lower here than in off-line traditional drug markets, but with the technological innovations follow new opportunities for stealing and fraud. The sites themselves fall prey to theft and hacking attempts, administrators abscond with users' funds, and malicious sellers regularly cheat buyers. In this study, we explore the types of theft and fraud that occur on cryptomarkets using multiple data sources: formalized community resources (e.g., guides, tutorials), ethnographic observations of user forums, thematic identification of forum posts using unsupervised text classification, and an expert interview. We find system-based violent predatory resource exchange similar to robberies and process-based fraudulent resource exchange similar to rip-offs. We discuss these offenses conceptually as extensions of common drug-related crimes in the digital world. This contributes to the research on how cryptomarkets work and can improve crime-prevention efforts.

Keywords

cryptomarkets, fraud, drug market interventions, crime prevention

[1]Aalborg University, Aalborg, Denmark
[2]University of Montreal, Montreal, Quebec, Canada
[3]University of Copenhagen, Copenhagen, Denmark

Corresponding Author:
Kim Moeller, Aalborg University, Kroghstræde 7, Aalborg 9000, Denmark.
Email: km@socsci.aau.dk

Introduction

Illicit drug markets exist in direct opposition to the state's regulation. Participants are routinely arrested and face severe criminal sanctions. Despite this, drug markets persist because buyers and sellers strategically adapt their transactions in ways that reduce the risk of law enforcement intervention and personal victimization (Moeller, Copes, & Hoechstetler, 2016). In recent years, these adaptations have increasingly involved moving transactions online to so-called cryptomarkets (Soska & Christin, 2015). Cryptomarkets are located on the "dark web" as hidden services using the Tor network (The Onion Router) and use encrypted communications and bitcoin to provide anonymity and security. Compared with illicit drug markets in the real world, cryptomarkets are anonymous and open but transcend physical locations (Aldridge & Décary-Hétu, 2016).

A growing research has examined these online exchanges and found that illicit drugs constitute the majority of transactions (e.g., Barratt, 2012; Christin, 2012; Martin, 2014; Soska & Christin, 2015; Van Hout & Bingham, 2013, 2014), secondarily to stolen data (e.g., Hutchings & Holt, 2014; Wehinger, 2011). A central finding in this research is that the risks of legal sanctions are low for both buyers and sellers as the whole cryptomarket ecosystem is highly resilient to interventions (Décary-Hétu & Giommoni, 2016; Soska & Christin, 2015; Van Buskirk et al., 2017; Van Buskirk, Roxburgh, Farrell, & Burns, 2014). So far, law enforcement efforts have primarily targeted the administrators of the sites, and buyers have been jeopardized only because of traditional police work, such as intercepting shipments in the mail (Europol, 2013).

The same technology that is designed to reduce the risk of being robbed or scammed also enables new forms of fraudulent behavior. At the system level, cryptomarkets are regularly exposed to theft and hacking attempts, and the bitcoin technology also has security flaws (Wehinger, 2011). At the process level, some vendors defraud buyers when shipping the drugs. The administrators of the sites work to alleviate these problems with several self-regulation mechanisms, such as buyer reviews, licenses, and authorizations for reliable vendors, banning malicious users, locking accounts, and implementing escrow services for payments. Despite these mechanisms, there are regular reports of theft and fraudulent behavior on online forums dedicated to cryptomarket discussions. These user forums are online communities where virtual offenders converge and have established their own norms, rules, and vocabulary (Martin, 2014; Soudijn & Zegers, 2012). User forums serve many different purposes for offenders, one of which is information dissemination to reduce the risks associated with the use of the postal system (Aldridge & Askew, 2017; Holt, Blevins, & Kuhns, 2014). The discussions on these forums constitute threads of individual posts that form conversations that are amenable to content analysis (Denzin, 1999; Williams & Copes, 2005), and several qualitative studies have used these data to examine various aspects of cryptomarkets (Aldridge & Askew, 2017; Bancroft & Reid, 2016; Martin, 2014).

In this study, we explore the different types of theft and fraud that occur in relation to illicit drug transactions on cryptomarkets, based on dark web forum data. The point of departure is Jacques and Wright's (2011) conceptualizations of illicit transactions as a combination of resource exchange and informal social control. Resource exchange

takes the form of reciprocation, altruism, or predation. Reciprocation is a regular sale where the price varies depending on the social distance between seller and buyer. Repeat customers may receive lower prices and friends may even altruistically receive drugs as gifts (Kandel & Davis, 1991; Moeller & Sandberg, 2015). Some sellers use predation to increase profits. Predatory resource exchange consists of violence, fraud, or stealth. Using Jacques and Wright's (2011) concepts, robbery (Jacobs, 2000) is a violent resource exchange while rip-offs are a fraudulent resource exchange (Jacques, Allen, & Wright, 2014). Cryptomarket administrators attempt to prevent this malfeasance through social control (Martin, 2014), conceptualized as conflict management and retaliation (Jacques & Wright, 2011). There is a dispute resolution system wherein grievances can be settled and administrators can also ban vendors and buyers who do not comply with the rules. These options for conflict management and retaliation are not always effective against motivated offenders and can even be counterproductive.

We employ a rational choice perspective to examine how offenders exploit weaknesses in the cryptomarket technology to defraud users. We assume that the actors are motivated, opportunistic, and weigh the subjective utility of alternative actions. They are not absolutely deterred by law enforcement or other threats but adapt their offending behavior strategically to less risky alternatives (Cross, 2000; Moeller et al., 2016). A similar theoretical framework has been used in the study of illicit off-line drug markets (Jacques & Wright, 2011), cybercrime (Yar, 2005), and markets for stolen data (Hutchings & Holt, 2014). We recognize there are other more emotional and less rational mechanisms at work on cryptomarkets, such as culture and politics (Maddox, Barratt, Allen, & Lenton, 2016; Munksgaard & Demant, 2016), but they are not the focus of this study.

In the section that follows, we review the research that examines the problems with predatory resource exchanges on cryptomarkets. These actions violently target the system-based infrastructure of the dark web, Tor, and Bitcoin, and fraudulently target the process-based reputation mechanism. Next, we introduce our methodology and data-collection procedures. In the findings section, we present the different forms of predatory resource exchange and discuss the parallels between these acts and the thefts and frauds that occur in off-line drug markets.

Review

This section outlines research that examines theft and fraud in online commerce. To gain a better understanding of these problems, we include research that has examined vulnerabilities in legal online peer-to-peer systems and bitcoin exchanges. We also include a number of non–peer reviewed references to strengthen the connection between online fraud and the dark web. We first describe the system-based control mechanisms and the violent predation that exploits them: DoS (denial-of-service) attacks, hacks, and bitcoin theft. Next, we describe how the reputation mechanism works to prevent fraudulent predation and provide examples of circumvention. Next, we describe the available methods for social control that site administrators apply in the form of conflict management and retaliation. Finally, we explain the "finalizing early" (FE) option that is the exception to these control mechanisms.

System-Based Control and Violent Resource Exchange

The cryptomarket infrastructure uses the anonymizing Tor network to operate as hidden services and uses bitcoin for transactions. Bitcoin is a virtual currency designed for online payments outside the traditional banking system (Böhme, Christin, Edelman, & Moore, 2015) and is the most popular method for payment on cryptomarkets (Europol, 2016). The Tor network is the preferred medium for cryptomarkets and ensures that the server cannot be physically located by law enforcement and that all communication is anonymized. Consequently, the sites operate with impunity with regard to the typical ensemble of techniques to contain illicit Internet activity (e.g., Goldsmith, 2000; Hutchings & Holt, 2014).

Hidden services and cryptocurrency have two general weaknesses. First, hidden services are vulnerable to DoS attacks that bombard a server with requests until it slows down and eventually goes offline (Wehinger, 2011). Paulson and Weber (2006) noted that DoS attacks are used as "cyber extortion" because they can take websites offline and demand ransoms before attacks are stopped. Mitigating DoS attacks is particularly difficult for hidden services (Tor Project, 2013, 2014).

Second is the bitcoin private key for transactions, which can be stolen from a website through hacking. A key characteristic of bitcoin is that transactions are irreversible, contrary to other forms of online payment (Böhme et al., 2015). This irreversibility is intended to prevent fraud but simultaneously makes bitcoins an ideal target for theft (Doguet, 2013). Once a bitcoin is stolen, it cannot be retrieved. The largest known bitcoin theft was of 850,000 bitcoins from the MtGox exchange in 2013 (Bradbury, 2013). Allegedly, MtGox was subjected to an exploitation of a vulnerability known as a "transaction malleability" flaw in the Bitcoin protocol. Subsequent analysis (Decker & Wattenhofer, 2014) found that only 386 (sic!) of the bitcoins that disappeared could be explained by this vulnerability. The investigation is still ongoing. Moore and Christin (2013) calculated a risk ratio for more than 40 bitcoin currency exchanges and found that larger exchanges were less likely to be shut down. Conversely, larger exchanges are also more valuable targets to thieves.

Cyber extortion and bitcoin theft target the system-based controls and cause damage, exert force, and apply coercion. Conceptually, we interpret these actions as violent resource exchange, similar to robberies (Jacobs, 2000; Jacques & Wright, 2011), even though they are directed at the digital infrastructure of the sites and not the physical integrity of the administrators. This interpretation departs from Yar's (2005) observation that the online context can be understood in the extension of the conventional routine activity concepts of distance, weight, and value.

Process-Based Control and Fraudulent Resource Exchange

Process-based control revolves around the review mechanism, also referred to as the reputation systems (Resnick, Kuwabara, Zeckhauser, & Friedman, 2000). The review mechanism is designed to sanction misbehavior while imposing minimal costs on well-behaved users, similarly to legal e-commerce sites such as eBay and Amazon

(Marti & Garcia-Molina, 2005). A variety of statistics (e.g., total sales, average review score) are published for each vendor pseudonym (e.g., "Xanax_King"), and with each transaction, buyers are encouraged, or even required, to provide a score for the product and the process. Kruithof et al. (2016) suggest that about 71% to 81% of cryptomarket transactions have an associated review, which is more than on eBay where only about half of the transactions are rated (Resnick, Zeckhauser, Swanson, & Lockwood, 2006). Buyers' number of transactions is also displayed to vendors and some may prioritize between customers, based on their history of giving favorable ratings (Van Hout & Bingham, 2014).

The weakness of the review mechanism is that the opinions of unknown peers affect others' decisions and the authenticity of these opinions cannot readily be ascertained. Manipulating reviews is a common form of fraud on legal online markets as well as cryptomarkets (Markopoulos, Xefteris, & Dellarocas, 2015). Known techniques include providing unfair recommendations and obtaining a positive reputation while strategically preparing to defect. Some vendors register multiple accounts, purchase their own stock, and leave good reviews. Others referred to as "whitewashers," leave or are banned, and then rejoin with new identities (Marti & Garcia-Molina, 2005).

Site administrators can influence reputations by awarding reliable vendors with a "verified status" (Wehinger, 2011). A verified status is achieved after a number of successful transactions and carries across different sites. This is important because vendors with a verified status can immediately continue on another site in case law enforcement or a DoS attack takes down a marketplace (Dolliver, 2015). Technically, verified status requires that participants cannot steal each other's identity, which is referred to as "spoof-resistance." Spoof-resistance is based on a cryptographic key that is uniquely associated with the pseudonym of a vendor (Koutrouli & Tsalgatidou, 2012).

According to Jacques and Wright's (2011) conceptualization, resource exchanges based on the false premise of manipulated reviews are predatory and fraudulent. The site administrators are aware of the fraudulent predation that takes place and seek to prevent it through various means of social control.

Social Control and the "FE" Exception

Cryptomarket administrators use different forms of social control to build trust between vendors and buyers and also actively engage with users on the forums (Martin, 2014). Following Jacques and Wright's (2011) conceptualization, we understand these social controls as conflict management and retaliation.

The most formal social control available to administrators is the centralized dispute resolution mode. If a package does not arrive, the buyer and seller can discuss refunds here with administrators as mediators and active conflict managers. The users in Van Hout and Bingham's (2013) study evaluated the dispute resolution mode positively, even though only a few had experience with using it. Site administrators also manage conflicts more informally when they participate on the forums and update users with

news of technical problems, such as DoS attacks or hacking attempts that explain downtime (Martin, 2014). This proactive conflict management prevents user speculations that the site might have more serious security problems.

In the case of problems with individual malicious vendors, administrators can retaliate by either banning or "doxxing" them. Banned vendors will have to acquire a new bond and start their reputation building anew using another pseudonym. Because of the start-up costs of building a reputation, this is a serious economic sanction (Resnick et al., 2006). Doxxing or "dropping dox" is a more severe form of retaliation and involves the publication of documents containing phone numbers, financial information, medical records, emails, and so forth. Administrators can retrieve this information from messages stored on the server, but they are hesitant in publishing it. Doxxing is controversial because it breaches the fundamental premise of anonymity that the entire cryptomarket community is based on (Bancroft & Reid, 2016; Maddox et al., 2016).

Finally, there is one exception to the system- and process-based control mechanisms that also eludes conflict management and retaliatory measures. When conducting transactions, there is an option to "finalize early" (FE). Finalizing early implies that the buyer pays for the product in advance, in contrast to the standard procedure of holding the payment in the escrow system until arrival has been confirmed. Some vendors will request or even require that buyers FE before proceeding with shipments. The rationale for accepting to FE is threefold. First, the bitcoin exchange rate is so volatile that fluctuations between shipment and arrival can sometimes mean the difference of making a profit (Moore & Christin, 2013). Second, there may be a fee to use the escrow service (Martin, 2014; Van Hout & Bingham, 2014). Third, the centralized escrow system is vulnerable, because hackers or even administrators may abscond with the funds. The pitfalls of FE are obvious, as bitcoin transactions are irreversible.

In the following section, we describe our methods and data collection procedures before proceeding with the findings, where we present the different types of violent and fraudulent resource exchanges in cryptomarkets.

Data and Method

Our primary data comprise forum threads where buyers, vendors, and administrators discuss cryptomarket issues. We found numerous threads where violent and fraudulent resource exchanges are critically disseminated along with discussions of the utility of the social control mechanisms. These threads are chronologically organized textual conversations that constitute cultural artifacts, amenable for empirical analysis (Williams & Copes, 2005). A number of studies have used online forum threads to examine various forms of offending (Aldridge & Askew, 2017; Bancroft & Reid, 2016; Holt et al., 2014; Martin, 2014), and the overall approach has been endorsed as "netnography" (Kozinets, 2002).

We use two complementary techniques to collect data from the threads, "lurking" and web crawling. Lurking is an element of observational ethnography (Garcia, Standlee, Bechkoff, & Yan, 2009) that has previously been applied in nethnographic

cryptomarket studies (Aldridge & Askew, 2017; Bancroft & Reid, 2016; Martin, 2014). We lurked user forums and actively monitored threads on the r/DarkNetMarkets subreddit on reddit.com for 18 months (between January 2014 and July 2015) with the aim of exploring various types of predatory resource exchanges. Forum posts that mentioned predatory resource exchange were copied and saved for later analysis. The researchers collectively discussed the contents of the posts and this led to the identification of the system- and process-based predatory resource exchanges.

The ethics of observational nethnography are not solidly defined (see Kozinets, 2002; Martin & Christin, 2016). Following previous research, we decided not to actively participate or seek approval of our lurking (Aldridge & Askew, 2017). We consider the settings we observe as more public than private, given that they do not require membership and the participant count is in the thousands (Eysenbach & Till, 2001). In addition, the persons under study are "pseudonymous" and not readily identifiable (see Bancroft & Reid, 2016, for a discussion of this concept).

Next, we supplemented this observational data with data collected through web crawling provided through a publicly available data set hosted by The Internet Archive (Branwen et al., 2015). We first extracted 2.6 million forum posts and processed them by removing non-English posts, short posts, stemming, and stop words. This reduced the corpus to 404,161 posts from six forums that contained a vocabulary of 4,688 terms that we then subjected to unsupervised text classification using topic modeling. Topic modeling provides an "automated procedure for coding the content of a corpora of texts (including large corpora) into a set of substantively meaningful coding categories called 'topic'" (Mohr & Bogdanov, 2013, p. 546). Specifically, we applied a correlated topic model (Blei & Lafferty, 2007) by using the *stm* package developed by Roberts, Stewart, and Tingley (2015). This procedure provides an estimated proportion of a document, in our case, a forum post, which can be assigned to a specified "topic". We found and reviewed 200 "exemplar documents" (Roberts et al., 2014) that contain high proportions of predatory resource exchange-related topics. Topic modeling is typically applied for quantitative purposes (Grimmer & Stewart, 2013), but we use it purely as a qualitative aid to identify relevant forum posts. The topic model allows us to navigate thousands of documents in order to find additional empirical material that complements the material we collected through "lurking." It provides an alternate entry point to predatory resource exchange-related content.

Third and finally, we conducted informant ethnography with a semistructured interview over email with DeepDotWeb, the author of the blog DeepDotWeb.com, from December 2014 to January 2015. DeepDotWeb.com hosts interviews with administrators and provides discussions and news regarding cryptomarkets. The interview schedule emerged from the initial observational ethnography. We presented DeepDotWeb with our initial analysis and he provided comments, further insight, and critical evaluations of some publicly known examples of system-based theft. On having completed our analysis, we discussed our findings with DeepDotWeb, thus improving external validity by consulting a community expert.

We have two ambitions with this methodological approach. First, we use the different forms of data collection (web crawling, lurking, and interviews) to ensure that we

are able to make detailed descriptions and not miss central aspects, referred to as convergence validity (Fielding, 2008). Second, we triangulate by taking the findings from the different data sources to position critical questions from other sources (Hammersley, 2008). Triangulation is based on the validation of findings from each method by comparing them to each other (Denzin, 1999). This pertains especially to our findings on system-based violent resource exchange that has previously only been established in grey literature and in statements made by administrators. Summing up, we use lurking to identify potentially relevant forms of predatory resource exchange. Next, we use topic modeling to secure these findings within a larger number of cases. Finally, the interview with an expert provides us with a critical perspective on our interpretations of the two initial data sets. The quotes we use are verbatim, including grammatical errors and jargon. Some of the quotes we use are now unavailable online, owing to Operation Onymous shutting down several cryptomarkets and their forums (Europol, 2014), while other marketplaces went offline during our research. We remain in possession of transcripts of forum threads, which are available on request to the authors.

Findings

In the sections that follow, we first present the predatory activities that are aimed at the sites themselves, broadly conceptualized as system-based violent resource exchange. Next, we explore the malicious activities that target users, conceptualized as process-based fraudulent resource exchange.

System-Based Violent Resource Exchange

Cryptomarkets compete for customers based on the robustness of their technological infrastructure, trustworthy administration, high uptime, and pleasant interfaces. This competition increased after the first Silk Road incarnation was taken down in 2014. Silk Road had a dominant market share and the ensuing vacuum sparked a series of new marketplaces. Paradoxically, the total use of cryptomarkets increased despite the negative media attention (Soska & Christin, 2015).

DoS Attacks and Hacking

Cryptomarkets are targeted at the system level by DoS attacks and hacking and several sites have publicized statements of being victims of DoS attacks, as well as hacks and subsequent theft (DeepDotWeb, 2013a, 2013b, 2013c, 2014a, 2014b, 2014c, 2014e, 2014f, 2014g, 2014h). DoS attacks render sites unusable for the purposes of extortion and competition. Some buyers displace their transactions while the site is down and this blocks income from commissions. DeepDotWeb explains the consequences of DoS attacks as follows:

> If Silk Road is down, everyone move to agora, if Agora is down, everyone moves to Evo . . . and so on [. . .] the DNM's users base is VERY herd like. (DeepDotWeb interview)

At the most direct level, this displacement is a matter of buyers wanting to conduct their transactions without delay; however, it opens for other venues of predation. Hackers can exploit the displacement effect and demand ransoms to stop the attack. From the trial against Ross Ulbricht, operator of the Silk Road marketplace, we know that he paid an extortion fee to both hackers and DoS attackers (Jackson, 2015). To what extent DoS attacks effectively spur migrations of buyers and vendors is not entirely clear. Many marketplaces have suffered DoS attacks and regular downtime but have managed to operate successful businesses nevertheless. For example, we note that the market Agora, known in communities for its frequent downtime, was one of the largest markets in operation at the time. Displacement does not necessarily mean migration to competitors. Users might strategically adapt in other ways (Moeller et al., 2016) and begin to source through offline connections or merely postpone their activities to a time when the market is operational.

We found some evidence suggesting that site administrators themselves have used DoS attacks as part of the intersite competition for customers. These intersite conflicts are not well understood and the forum posts that address them are shrouded by various conspiracy theories and wild speculation, as exemplified by these posts:

> Those are the theories you came up with? Remember when DPR thought Backopy was running Utopia using the name SWIM? Now who is it who runs a deepweb market using different names? Remember when DPR said he had evidence that Tormarket was behind a DDOS attack on SR2 when Tormarket was the main competitor of SR2? So who could be behind a DDOS attack on SR2's main competitor? (Agora Marketplace forums, March 9, 2014)

> [Sheep Marketplace] did not have these problems and quickly became the top site on the deepweb, then stole everyone's bitcoin. I think the sheepfuckers are the same people behind tormarket, and are again sending a DDOS attack against their number 1 competitor SR2.0 Just my theory. (Silk Road 2.0 forums, December 17, 2013)

In one confirmed case, intersite competition led to the exploitation of security vulnerabilities with hacking tools known from regular cybercrime. These attacks consist of gaining access to databases with information on incriminating and illegal acts, which may include unencrypted addresses of inexperienced users and bitcoins. This can also be used for extortion or as a form of competitive violence, where the perpetrators delegitimize their competitor's site by first exploiting and then publishing their security vulnerabilities. In December 2013, a hacker gained access to the TorMarket database. TorMarket had branded itself on having high security and the breach was detrimental to the integrity of the administrators (DeepDotWeb, 2013b). The then administrator, Dread Pirate Roberts, published the TorMarket hack on the Silk Road 2.0 forums and presented database information to expose his competitor's vulnerabilities. DeepDotWeb explains the severity of such incidents:

> Security flaws are the most unforgivable "crimes" in the DNM world. from obvious reasons—losing money, leaking personal details, LE [. . .] If an admin fails to react,

> admit and fix the issue quickly without losing money, its a death certificate for a market. (DeepDotWeb interview)

Two other, less well-documented, cases of intersite violence consisted of a moderator hiring outside help to post child sexual exploitation material on a competitor's forum. This was allegedly for revenge, as the competitor had advertised on the Silk Road 2.0's forums (Klippenstein, 2014). Anecdotally:

> I knew something wasn't right. Clu supposedly (extremely high probability) posted CP on another site. AND Clu is a scumbag site operator. Alfred knows this. (The Hub forums, May 9, 2014)

Where DoS attacks are quite common, hacking competing marketplaces is less used. In our interview, DeepDotWeb argues that Operation Onymous (Europol, 2014) may have further reduced this type of competition between marketplaces. Site administrators are now focused on improving their own security, instead of fighting competitors. Since the confirmed cases of DoS attacks and the hack and subsequent publication of data from TorMarket, we have not witnessed any similar events discussed on the forums. Empirically, it does not appear to be a widespread phenomenon, but we acknowledge that such actions may not be publicized because of public relations concerns of the specific marketplace. However, we note that the perpetrators of the other acts of violence than DoS attacks were all associated with Silk Road 2.0, which was shut down during Operation Onymous.

Bitcoin Heists and Marketplace Exit Scams

Bitcoin heists and marketplace exit scams are violent forms of predatory resource exchange that are both directed at the system-level of cryptomarkets. The centralized nature of cryptomarkets implies that funds amass in the escrow system. The irreversibility of transactions, and the pseudonymous and anonymizable properties (for a discussion of these terms, see Bancroft & Reid, 2016), makes bitcoin a perfect target and large sums can be transferred across the globe instantaneously (Yar, 2005). Furthermore, bitcoin theft, as with hacking, constitutes a security breach and creates mistrust in the site, which can displace users. In this sense, the consequences of a bitcoin heist are twofold. We refer to bitcoin theft as "heists" if they are perpetrated by an outside party and "marketplace exit scams" if perpetrated by administrators or other insiders. The term *exit scam* has other meanings as well (described in the section below); hence, "marketplace" was added to better capture the system-level characteristics of this particular act.

In February 2014, US$2.7 million in bitcoin was stolen from Silk Road 2.0. According to DEFCON, who was administrator at the time, a hacker exploited a vulnerability in the Bitcoin protocol while a new tumbling system was being implemented (DeepDotWeb 2014c; see also Decker & Wattenhofer, 2014):

> Our initial investigations indicate that a vendor exploited a recently discovered vulnerability in the Bitcoin protocol known as "transaction malleability" to repeatedly

> withdraw coins from our system until it was completely empty. (DEFCON, Silk Road 2.0 forums, February 13, 2014)

The prevailing sentiment in the cryptomarket community, however, is that this heist was a marketplace exit scam where the site administrators stole the funds themselves:

> It definitely could be an inside job. When the hack originally occurred, an inside job was one of the leading theories. The Dev Teams broken promises and lack of action since that time does make the possibility of an inside job/long con seem more plausible. (Silk Road 2.0 forums, October 5, 2014)

> I firmly believe that the jan hack inside job, multi sig escrow a ploy to keep buyers loyal to the site, defcon doesnt need to ingrate it i imagine this site gets enough new buyers from the media scaremongering, many of whom are new to the scene and know no better. i leave with you a question, if your partner stole from you, gave you empty promises and ignored your concerns how long would you stick around for out of blind loyalty? (Silk Road 2.0 forums, October 10, 2014)

> I personally think that Defcon is a thief. If he is not a thief, then he is incompetent. Either way he is not qualified to run a black market website. (Silk Road 2.0 forums, February 16, 2014)

In the first and third examples, the users' postings connect the heists, which may as well have been marketplace exit scams, to the qualifications of the administrators. This twofold damage in the form of financial loss, and loss of trust in the administration to properly operate the site, is illustrated in the following quote. Discussing the Silk Road 2.0 alleged bitcoin heist, DeepDotWeb explained:

> I disagree with the term "hack"—and i would define it as "inside theft" Defcon? DPR2? another Developer? [. . .] Everything in the chain of events before this so called "hack" and surely after that, leads us to this conclusion. The lying, the fake repayment process, the lack of escrow, the stealing mods, the stupid psyops. (DeepDotWeb interview)

There are several other known examples of bitcoin heists against markets such as Black Market Reloaded, Pandora Marketplace, and Cannabis Road (DeepDotWeb, 2013a, 2014a, 2014b). Interestingly, these examples are also commonly perceived to be marketplace exit scams in the cryptomarket community (DeepDotWeb, 2015b). Discussing centralized escrow solutions, one user mocks the naivety of a peer by listing the cryptomarkets who recently lost user funds to bitcoin heists, marketplace exit scams, or law enforcement intervention:

> Are you fucking retarded? Let's look statistically at all past marketplaces
> Sheep: stole all coins
> Budster: stole all coins
> Sr 2.0: stole all coins

> BMR: Retired somewhat disgracefully after a database leak etc. etc. but Backopy was honorable
> Atlantis: Stole all coins
> SR 1.0: Law enforcement stole all of the coins
> Deepbay: Stole all of the coins
> Project Black Flag: Stole all of the coins
> Hey I wonder if Agora and Pandora will be different? WAKE THE FUCK UP PEOPLE TRUST BASED ESCROW IS OVER. MULTISIG is the WAY TO GO. (Silk Road 2.0 forums, February 14, 2014)

With Evolution Marketplace, a moderator confessed to the community that the administrators had indeed absconded with funds, making it the largest marketplace exit scam to date worth an estimated US$12 million (DeepDotWeb, 2015b). In the case of both Pandora Marketplace and Silk Road 2.0, administrators did not shut down the market but kept the scam going by lying to users about repayment plans. According to DeepDotWeb,

> This Was a scam site all along, money lost, vendors locked out, than "the hack"—and after that and the lies about the repayment that never took place (After increasing the market commission to 24%!!), locked out all vendors, disabled withdrawals and kept operating for another few months until it was finally taken down during Onymous. along with many other scam sites. (DeepDotWeb interview)

Discrepancies in the official stories are not lost on the users who will criticize and dissect the events and explanations on forums. In the second citation below, a user refers to expert knowledge on the security breach that allegedly allowed the theft of escrow funds and argues that the technical explanation does not hold up to scrutiny, concluding that either incompetence or malice are the only possible explanations:

> ITS FUCKING PLAIN AND SIMPLE ESCROW SYSTEM WAS A SCAM SO EVERY COCKSUCKER WHO DIDNT FINALZE THE COINS STAYED IN THE BANK AND OPPS WE HAVE BEEN HACKED. (Silk Road 2.0 forums, February 17, 2014)

> SR2 has recently had 2 incidents in which funds in escrow were stolen. Here are the facts as we know them. 1. In the latest theft over 5000 bitcoins were stolen. More than double the amount that SR staff has admitted to being stolen. 2. SR staff have blamed the theft on hackers. Many people knowledgeable about the bitcoin protocol find the theft of all the coins held by SR through transaction malleability to be implausible. 3. If hackers did in fact manage to steal from SR users, then the SR administration is extraordinarily incompetent. (The Hub forums, February 14, 2014)

These system-based violent predatory resource exchanges are not well-understood by the users of cryptomarket forums. Users discuss and dissect motives and technical explanations, but have no way to verify whether hackers or marketplace owners stole funds, as marketplace owners may well-blame heists on hackers. The general

sentiment is skepticism toward the explanations put forth by site administrators, but the actual attribution of responsibility is difficult, if not impossible. The result is speculative and conspiracy-oriented posts:

> Silkroad 2.0 was compromised the day it was hacked and since then it was being run by Feds to gather info. The coins which were hacked from silkroad ended up In the Gov auction and it was a trap from that day on. [. . .] Feds are running other markets too so Please stick to Agora and Stay Safe. (Agora Marketplace forums, November 7, 2014)

Though the architectures of cryptomarkets and bitcoin technology are designed to ensure anonymous transactions, it also opens up new ways to exploit the lack of legal recourse in illicit markets. Our findings suggest that the fear expressed by users in Van Hout and Bingham's (2013) study was well-warranted. There are fundamental vulnerabilities at the system level of the cryptomarket infrastructure. However, where Van Hout and Bingham's (2013) interviewees were mostly concerned with the risk of law enforcement exploiting the technology, in our data, the users were more worried about malicious peers.

Process-Based Fraudulent Resource Exchange

The reputation system creates a type of fraudulent resource exchange that revolves around unreliable feedback and fake accounts. Vendors can leave negative reviews for competing vendors and a good reputation can be used to convince buyers to finalize early, rather than use escrow. There are several guides available to new users on how to avoid being defrauded (see, e.g., Reddit, 2014a, 2014b). The two most common forms of fraudulent predation can be conceptualized as "exit scams" and "selective scams," which is the terminology used by community members themselves.

Exit Scams

In exit scams, malicious vendors build up a good reputation and then suddenly defect, taking the funds from un-dispatched but finalized orders. The forums abound with examples. This particular forum member describes the process in detail:

> Almost everyone that ordered with DaRuthless before he pulled his exit scam were satisfied too. The scam is:
>
> 1) Operate as a good vendor for x months, building up high vendor ranking
>
> 2) Come up with some excuse or another that orders have to be FE'd
>
> 3) Keep the proceeds from all the FE orders without shipping any product, for as long as you can keep it going
>
> 4) Start a new vendor account—go to step 1
>
> So it's nice you guys had a good experience with Divine, but that doesn't prove whether or not he is a reincarnation of DaRuthless. (Silk Road forums, August 4, 2013)

The exit scam is best exemplified in what Ormsby (2012, "Meet Tony76") referred to as "The Great 4/20 Scam." In 2012, "Tony76," a vendor on the original Silk Road with an excellent reputation, celebrated 4/20 by offering his products at low prices. Demand for Tony76's product soared and he asked users to finalize early with reference to the many orders. When users started complaining that their products did not arrive, Tony76 had already disappeared.

Some forum members describe exit scams as regular events and write in a tone as if they were teaching less cryptomarket literate members of the informal workings of the markets. In this way, they produce a language of cryptomarkets by establishing exit scams as an everyday concept:

> But even that can backfire as trusted vendors have turned rogue with no warning now. Many of them have done this. How is one supposed to know that the vendor has decided to pull an exit scam? Without escrow of some type, buyers have little real protection against scamming. (Silk Road 2.0 forums, April 18, 2014)

> Fent—I am new as well. IMO, I will never FE even for established vendors. Look at what is happening with this guy Baron on this site and others. From what I understand, he has had a solid rep. for a long time. Now, has ripped off people for thousands of dollars. I think they are calling it an exit scam—he is quitting the business and has decided to rip off all of his customers on the way out. However, he may not even be quitting. He could simply open up another vendor account under another name and start selling again. Bottom line is that if you FE, you are asking to be ripped off. (Evolution Marketplace forums, January 23, 2015)

Exit scams rely on the reputation of the vendor and the associated ability to have users finalize early. When these scams end, the perpetrators can whitewash and start anew. The profitability depends on the vendors' ability to keep the scam going, but they are known to be profitable, as a former vendor professed in a post:

> In two weeks I had made enough coins for a down payment on a house and I was going to use it exactly for that. (DeepDotWeb, 2014d)

Users are well-aware of the risk and, as one elaborates, the key to the exit scam is building up a customer base and reputation.

> I don't know any scammer that asked FE straight away and managed to scam properly but ketosaurus. The most dangerous scams are when vendors have a solid customer base. If this vendor wanted to scam now he would make barely 1k, if he scams in a couple month when he has a huge customer base he would make at least 20 times more. (Agora Marketplace Forums, November 11, 2014)

Users speculate on the existence of serial exit scammers, like the whitewashers in markets for stolen data (Marti & Garcia-Molina, 2005). However, as the quote below illustrates, serial exit scammers suffer under the fact that they have to give up

information on shipping. If a vendor who has previously exit scammed attempts to rebuild his business under a new pseudonym, subtle clues such as shipping area, writing style, and packaging allow buyers to identify previous malicious actions.

> Does anyone know the whereabouts TwistyTheClown's general location? I ask this in order to be sure if he comes under a new alias I can see if it's him . . . these exit scammers go through a cycle of making a vendor account . . . acquire good rep with good product/escrow, few weeks/months later they exit scam, then they repeat this process under a different vendor name. (Evolution Marketplace forums, February 14, 2015)

It is important to note that buyers, as the one above, have to visit forums to be aware of fraudulent predation (see also Holt et al., 2014). Newcomers and less active members are less likely to be aware of information on impending exit scams or how scammers operate.

Selective Scams

The selective scam is an on-going venture where vendors refrain from shipping a fraction of total purchases but maintain that they have been shipped. This appears to be a widespread practice as evidenced by the almost daily allegations on the forums. DeepDotWeb explains the logic of its continuation as such:

> If a vendor have large sales volume and out of this volume he will intentionally scam some % of the buyers, he will get away with it easily. lets assume he will scam 1%-5% of his buyers, that have no high "buyer stats" he can get away with it always. (DeepDotWeb interview)

Instead of sending products, vendors may ship empty packages, low quality, impure, or fake products and refund only a percentage of the value (see, e.g., Reddit, 2014a). Vendors can also stall allegations of scamming by sending fake custom notices, referred to as "love letters," or by referring to other practical problems such as difficulties procuring products and the inherent problems of shipping drugs in the mail. If vendors are successful, the scam continues for weeks and even months. In one example, a vendor provided excellent service and product for the first shipment and then performed horribly on the second buy:

> Powder definitive stepped, almost street gear really weak quality compared to first order. (Evolution Marketplace forums, October 23, 2014)

Another user exemplifies this uncertainty in a discussion of his success rate:

> I have made 70+ orders and i have gotten every item ive ever ordered, with the exception of 1 scam who was trusted vendor that intentionally scammed people using his reputation. and one other package that the vendor provided the tracking number for which for some odd reason was Undeliverable as addressed. neither of our faults. (Silk Road 2.0 forums, March 12, 2014)

The user describes that the package could not be delivered and noted that this was probably an issue in the postal system. However, this event follows the exact methodology for selective scamming laid out in a community guide (Reddit, 2014a), wherein vendors send an undeliverable package to the buyer's zip code. The package is then "lost" but the buyer has no recourse as the vendor can provide shipping information if the buyer seeks moderators to mediate a dispute.

This final stage of the transaction is the most precarious. The buyer is exposed to law enforcement intervention at a physical location (Yar, 2005). Some advocate the use of PO boxes and some recommend using personal addresses as they are less suspicious (DeepDotWeb, 2015a; Reddit, 2015). When buyers reveal their home addresses as shipping destinations, they also provide malicious peers with a lever for extortion. This breach of anonymity has been used to ensure positive reviews through doxxing threats and users sometimes publish the threats made by vendors:

> Well, this turned out to be a fucking nightmare. This vendor is a complete prick, made up every excuse in the book and went as far as to THREATEN MY LIFE multiple times. They claim in numerous emails they kept my address and to watch my back if I didn't alter my negative feedback. (Reddit, September 7, 2014)

This dilemma succinctly illustrates the tension in the cryptomarket construct between desired anonymity and practical resource exchange. This relates to the utility of retaliation. A member of the vendor group, The Scurvy Crew, posted personal information on a user that had been a nuisance on the Agora Marketplace forum. The Scurvy Crew was banned and the administrator(s) of Agora Marketplace referenced the site rules and explained their actions with the statement: "Anonymity is sacrosanct here" (Agora Marketplace Forums, 2014). In another example, a moderator intervened when a vendor attempted to blackmail a buyer:

> The ex-vendor in question was found to have threatened a buyer with sending them a package and alerting Law Enforcement to it, and admitted making such a threat in an attempt to \"scare the buyer\" into paying for a package that he insisted had arrived. (Silk Road forums, June 11, 2013)

As described previously, moderators and administrators exercise conflict management and social control on cryptomarkets; much of this is related to process-based fraud. Moderators and administrators have privileged access to communication, if unencrypted, historical transaction records, and other information, and are capable of making as "fair" judgments as possible. In one example, a moderator summarized and publicly presented evidence that a buyer was trying to blackmail a vendor:

> It was removed due to you attempting to blackmail the vendor. I received a ticket from TopShelf420 regarding your behavior on September 25th. This complaint included messages sent from you that suggested blackmailing the vendor. The item relating to your complaint has received nothing but positive feedback throughout it's sale. Including positive feedback as recent as September 26th. Not only did you try and blackmail

> TopShelf420, but also you fabricated messages that were investigated by an Admin relating to threats in which you alleged DrBlackHat threatened to get law enforcement to your place of residence. This was also found to be false. Quite frankly your behavior thus far on both the market and the forums has been irrational and your complaints have been found to be false. (Evolution Marketplace forums, September 28, 2014)

Discussion

In this study, we examined the different types of predatory resource exchange that take place on cryptomarkets. This predation challenges the idea that illicit drug transactions on cryptomarkets are a low risk-free endeavor. These malicious peers exploit vulnerabilities in the technological infrastructure of the Tor network, the irreversibility of Bitcoin transactions, the use of feedback, whitewashing, and the inherent uncertainty associated with sending illicit drugs in the mail. Our findings indicate that users perceive them as more of a threat than law enforcement. Below, we discuss how the different forms of predatory resource exchange share characteristics with the violent and fraudulent resource exchange known from research on the off-line illicit drug market.

We found that DoS attacks are used against cryptomarkets for inter-site competition and extortive purposes. This has the direct effect of displacing users while the site is down and an indirect effect in revealing security breaches and delegitimizing administrators. We understand these attacks as parallel to the competitive systemic violence applied in off-line drug markets. Here, violence is used to displace buyers in the struggle for market shares. This displacement follows from the same restrictively deterrent adaptations that may have led buyers to cryptomarkets in the first place. Buyers are not absolutely deterred from committing illegal transactions in the face of risks but motivated offenders find less risky ways of continuing their offending (Holt et al., 2014; Moeller et al., 2016). The uncertainty that is created around a marketplace when it is targeted by hackers or DoS attacks is parallel to the perception of a risky transaction in an off-line marketplace that is targeted by violence. In our interview, DeepDotWeb described a development where administrators increasingly focus on improving their own sites rather than attacking others. This is consistent with the limited use of competitive violence in off-line drug markets where it is perceived as costly in terms of time and organizational resources (Moeller & Sandberg, 2015). It is generally more rational to maintain peace around illicit drug transactions.

While DeepDotWeb and forum members argued that security flaws were unforgivable crimes, we suggest a change has occurred since early 2015 when the interview took place. Now, there appears to be a fundamental conflict between the realities of the cryptomarket ecosystem on the one hand and the normative ideals of secure infrastructure on the other, of which the latter is connected to the cipherpunk and crypto-anarchist ethos on the forums (Maddox et al., 2016; Munksgaard & Demant, 2016). In April of 2016, AlphaBay, which is the largest marketplace in operation (Kruithof et al., 2016), leaked thousands of private messages between users (Cox, 2016). While no newer quantitative data on market sizes after the leak is available, AlphaBay is still in operation and is seemingly one of the biggest markets. Security flaws used to be an

unforgivable crime but do not seem to have the same implications for site credibility anymore.

The next form of predatory resource exchange we explored was bitcoin heists and marketplace exit scams. The centralized transaction system with escrow and user accounts (though some have implemented more secure multi-signature transactions) imply the sites are exposed to hackers that exploit the vulnerability of web applications and the irreversibility of Bitcoin transactions. The off-line parallel is the robberies of drug dealers that Jacobs (2000) analyzed. Victimized drug dealers have no legal recourse or way to recoup their loss and this makes them suitable targets. Similarly, cryptomarket administrators, buyers, and vendors cannot have their bitcoin insured because they engage in illicit activities. In the offline markets, victimized drug sellers exert social control and retaliate against wrongdoers (Jacques & Wright, 2011), but using violence is costly and prevents them from recouping their losses (Moeller & Sandberg, 2015). The exposure to bitcoin heists and the lack effective redress implies that cryptomarkets face a structural problem to their limits of growth. If they grow too big, they will attract too much attention from law enforcers and competitors. Similarly, the largest bitcoin exchanges are more exposed to hacking attempts (Moore & Christin, 2013). There may be an optimal size for cryptomarkets that is a function of the vulnerabilities in the system, parallel to how offline drug sellers constantly balance their security and visibility (Moeller et al., 2016).

An interesting twist to the examples of violent predation is the allegations that the administrators themselves perpetrated the heists. Assuming these consistent—albeit not well-documented—accusations are correct, there is no immediate parallel to predatory acts in offline drug markets. However, we note that there is some similarity with credit processes in illicit drug distribution. Higher-level distributors front drugs to lower-level distributors with promises of later repayment. At times, this repayment fails and the creditor cannot retaliate violently every time. Instead, the creditor sometimes accepts a loss as a cost of doing business (Moeller & Sandberg, 2015). The marketplace exit scams, are comparable except the direction of the victimization is inverse, so to speak. Cryptomarket buyers front the payment to administrators that act as a third party by way of the escrow system. When the drugs arrive, the vendor receives the payment. Hence, the escrow system has the same benefits and costs as credit in illicit drug distribution: it lubricates transactions and poses and resolves issues of trust.

We also examined process-based predation that we conceptualized as exit and selective scams. These fraudulent resource exchanges exploit the time lag when drugs go through the postal system (Aldridge & Askew, 2017). This temporal delay creates a room for maneuvering where the malicious peers operate. The review mechanism solves many problems with rip-offs known from the real world; however, it is vulnerable to whitewashers and fake feedback stemming from coercion or fraud. We found that users in cryptomarkets are acutely aware of this and actively discuss how to avoid being defrauded. This is a question of acquiring reliable information that introduces a distinction between experienced and less-experienced cryptomarket users. Experienced users are active on the forums and access this information (Holt et al., 2014). The

parallel here is that rip-offs in off-line drug markets are determined by social status and social distance. Strangers and addicts are the targets for predation (Jacques et al., 2014). This notion of social distance based on experience echoes Yar's (2005) observation that cybercrime can be understood as extensions of crime in the real world. An interesting quality of cryptomarkets is that vendors can also review customers. This provides a formalized method for discriminating between experienced and inexperienced buyers. This could spill over into the buyer's profile and lead other vendors to discriminate; it also illustrates how social distance and status become formalized on cryptomarkets.

Finally, the question of social control is a common thread in the different types of predatory resource exchange we have examined. The formal dispute resolution mode is an example of conflict management as social control (Jacques & Wright, 2011), but retaliation is more interesting analytically. Site administrators can retaliate against malicious peers by banning or doxxing them, which is comparable to nonviolent and violent retaliatory forms, respectively. Banning users is immediately effective, but it is a short-term solution. These users can whitewash and start over with a new identity shortly after. Doxxing pseudonyms is a practice that is deemed unacceptable by both community and site administrators. However, in some instances where many individuals are at risk, doxxing has been accepted by the community. Similarly, the norms against snitching in illicit drug markets are strong. The normative transgression associated with revealing information to legal authorities makes it a heavily sanctioned form of retaliation in offline drug markets (Moeller & Sandberg, 2015; Wehinger, 2011). This goes back to the parallel on the importance of maintaining peace in drug markets (Jacques & Wright, 2011). Retaliation is costly because it takes resources away from running the organization and it also creates enemies. In principle, cryptomarket administrators could use doxxing against particularly problematic vendors but we have not found examples of this practice in our data.

Conclusion

Our study contributes to the research on online illicit drug distribution by exploring problems with predatory resource exchange that are well-known to cryptomarket users but have not been analyzed separately. We identified primary types of violent predatory resource exchanges that affect cryptomarkets and their users: DoS attacks, bitcoin heists, and marketplace exit scams. DoS attacks exploit technological vulnerabilities and have been used against cryptomarkets with the purpose of extortion and displacing users to other sites. They may also function as a tool in intra-market competition. In bitcoin heists, hackers exploit the irreversibility of Bitcoin transactions and the vulnerability of web applications. An interesting perspective on these forms of predation was the widespread allegations, that these attacks and heists may have been perpetrated by the administrators of the sites themselves, which we conceptualized as marketplace exit scams.

Next, we examined the fraudulent resource exchanges that are process-based and conceptualized as exit and selective scams. These fraudulent exchanges exploit the

temporal lag in transactions. The drugs must go through the postal system, which gives malicious peers time to keep operating under a guise of legitimacy. We found that the reputation mechanism is vulnerable to fake feedback and that this feedback may even stem from coercion. The parallel here is that rip-offs in off-line drug markets are determined by social status and social distance, where strangers and addicts are the targets for predation. Social distance in our study is measured by experience with navigating cryptomarkets. The combination of encrypted communication, non-traceable payments, and shipping that contains a temporal delay to the completion of the transactions, amount to "the perfect condition to scam" (DeepDotWeb, interview). The asymmetry of information between the seller and buyer in offline drug markets was supposed to disappear on cryptomarkets. Instead, it has manifested in new, yet, parallel forms.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*, *41*, 101-109.

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, *35*, 7-15.

Bancroft, A., & Reid, P. S. (2016). Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. *International Journal of Drug Policy*, *35*, 42-49.

Barratt, M. J. (2012). Silk Road: eBay for drugs. *Addiction*, *107*, 683-683.

Blei, D. M., & Lafferty, J. D. (2007). A correlated topic model of science. *Annals of Applied Statistics*, *1*, 17-35.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, *29*, 213-238.

Bradbury, D. (2013). The problem with bitcoin. *Computer Fraud & Security*, *11*, 5-8.

Branwen, G., Christin, N., Décary-Hétu, D., Andersen, R. M., StExo, & Presidente, E. W. (2015). *Dark net market archives, 2011-2015*. Retrieved from www.gwern.net/Black-market%20archives

Cox, J. (2016, April 2). *Vulnerability in huge dark web marketplace exposes private messages*. Retrieved from https://motherboard.vice.com/en_us/article/vulnerability-in-huge-dark-web-marketplace-exposes-private-messages-alphabay-reddit

Decker, C., & Wattenhofer, R. (2014). Bitcoin transaction malleability and mtgox. In M. Kutyłowski & J. Vaidya (Eds.), *Computer Security—ESORICS 2014* (pp. 313-326). Cham, Switzerland: Springer International.

Décary-Hétu, D., & Giommoni, L. (2016). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, *67*, 1-21.

Denzin, N. (1999). Cybertalk and the method of instances. In S. Jones (Ed.), *Doing Internet research: Critical issues and methods for examining the Net* (pp. 107-125). Thousand Oaks, CA: Sage.

Doguet, J. J. (2013). *Nature of the form: Legal and regulatory issues surrounding the bitcoin digital currency system*. Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/louilr73&section=38

Dolliver, D. (2015). Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *Internal Journal of Drug Policy*, *26*, 1113-1123.

Europol. (2013). *Threat assessment (abridged)—Internet facilitated organized crime. iOCTA*. The Hague, Netherlands: Europol Public Information, European Police Office.

Europol. (2014, November 7). *Global action against dark markets on TOR*. Retrieved from https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network

Europol. (2016). *IOCTA 2016—Internet organized crime threat assessment*. The Hague, Netherlands: Europol Public Information, European Police Office.

Eysenbach, G., & Till, J. E. (2001). Ethical issues in qualitative research on internet communities. *British Medical Journal*, *323*, 1103-1105.

Fielding, N. (2008). Analytic density, postmodernism, and applied multiple method research. In M. M. Bergmann (Ed.), *Advances in mixed methods research* (pp. 37-53). London, England: Sage.

Garcia, A. C., Standlee, A. I., Bechkoff, J., & Yan, C. (2009). Ethnographic approaches to the Internet and computer-mediated communication. *Journal of Contemporary Ethnography*, *38*, 52-84.

Goldsmith, J. (2000). Unilateral regulation of the Internet: A modest defence. *European Journal of International Law*, *11*, 135-148.

Grimmer, J., & Stewart, B. M. (2013). Text as data: The promise and pitfalls of automatic content analysis methods for political texts. *Political Analysis*, *21*, 267-297.

Hammersley, M. (2008). Troubles with triangulation. In M. M. Bergmann (Ed.), *Advances in mixed methods research* (pp. 22-36). London, England: Sage.

Holt, T. J., Blevins, K. R., & Kuhns, J. B. (2014). Examining diffusion and arrest avoidance practices among Johns. *Crime & Delinquency*, *60*, 261-283.

Hutchings, A., & Holt, T. J. (2014). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*, 596-614.

Jackson, J. (2015). Silk Road paid thousands in shake-downs from malicious hackers. *Computerworld*, January 28. Retrieved from https://www.computerworld.com/article/2877052/silk-road-paid-thousands-in-shake-downs-from-malicious-hackers.html

Jacobs, B. A. (2000). *Robbing drug dealers: Violence beyond the law*. Piscataway, NJ: Transaction.

Jacques, S., Allen, A., & Wright, R. (2014). Drug dealers' rational choices on which customers to rip-off. *International Journal of Drug Policy*, *25*, 251-256.

Jacques, S., & Wright, R. (2011). Informal control and illicit drug trade. *Criminology*, *49*, 729-765.

Kandel, D., & Davies, M. (1991). Friendship networks, intimacy, and illicit drug use in young adulthood: A comparison of two competing theories. *Criminology*, *29*, 441-469.

Klippenstein, K. (2014, October 6). *What it's like to work for a darknet kingpin*. Cambridge, MA: Ars Technica. Retrieved from http://arstechnica.com/tech-policy/2014/06/punching-the-clock-for-a-darknet-kingpin/

Koutrouli, E., & Tsalgatidou, A. (2012). Taxonomy of attacks and defense mechanisms in P2P reputation systems—Lessons for reputation system designers. *Computer Science Review*, *6*, 47-70.

Kozinets, R. V. (2002). The field behind the screen: Using netnography for marketing research in online communities. *Journal of Marketing Research*, *39*, 61-72.

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands*. Santa Monica, CA: RAND Corporation.

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital "demimonde." *Information, Communication & Society*, *19*, 111-126.

Markopoulos, P., Xefteris, D., & Dellarocas, C. (2015). *Manipulating reviews in dark net markets to reduce crime*. Paper presented at the conference on Information Systems and Technology, Philadelphia, PA.

Marti, S., & Garcia-Molina, H. (2005). Taxonomy of trust: Categorizing P2P reputation systems. *Computer Networks*, *50*, 472-484.

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the "cryptomarket." *Criminology & Criminal Justice*, *14*, 351-367.

Martin, J., & Christin, N. (2016). Ethics in cryptomarket research. *International Journal of Drug Policy*, *35*, 84-91.

Moeller, K., Copes, H., & Hoechstetler, A. (2016). Advancing restrictive deterrence: A qualitative meta-synthesis. *Journal of Criminal Justice*, *46*, 82-93.

Moeller, K., & Sandberg, S. (2015). Credit and trust: Management of network ties in illicit drug distribution. *Journal of Research in Crime and Delinquency*, *52*, 691-716.

Mohr, J. W., & Bogdanov, P. (2013). Topic models: What they are and why they matter. *Poetics*, *41*, 545-569.

Moore, T., & Christin, N. (2013, April). *Beware the middleman: Empirical analysis of bitcoin-exchange risk* (Lecture Notes in Computer Science). Paper presented at the 17th international conference, Financial Cryptography and Data Security FC 2013, Okinawa, Japan.

Munksgaard, R., & Demant, J. (2016). Mixing politics and crime: The prevalence and decline of political discourse on the cryptomarket. *International Journal of Drug Policy*, *35*, 77-83.

Ormsby, E. (2012). *The Great 420 scam*. Retrieved from http://allthingsvice.com/2012/05/30/the-great-420-scam/

Paulson, R., & Weber, J. (2006). Cyberextortion: An overview of distributed denial of service attacks. *Issues in Information Systems*, *7*(2), 52-56.

Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation systems. *Communications of the ACM*, *43*, 45-48.

Resnick, P., Zeckhauser, R., Swanson, J., & Lockwood, K. (2006). The value of reputation on eBay: A controlled experiment. *Experimental Economics*, *9*, 79-101.

Roberts, M. E., Stewart, B. M., & Tingley, D. (2015). *stm: R package for structural topic models*. Retrieved from http://www.structuraltopicmodel.com

Roberts, M. E., Stewart, B. M., Tingley, D., Lucas, C., Leder-Luis, J., Gadarian, S. K., & Rand, D. G. (2014). Structural topic models for open-ended survey responses. *American Journal of Political Science*, *58*, 1064-1082.

Soska, K., & Christin, N. (2015). *Measuring the longitudinal evolution of the online anonymous marketplace ecosystem*. In *Proceedings of the 24th USENIX Conference on Security symposium* (pp. 33-48). Washington, DC: USENIX Association.

Soudijn, M. R., & Zegers, B. C. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, *15*, 111-129.

Van Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S., & Roxburgh, A. (2017). The recovery of online drug markets following law enforcement and other disruptions. *Drug and Alcohol Dependence*, *173*, 159-162.

Van Buskirk, J., Roxburgh, A., Farrell, M., & Burns, L. (2014). The closure of the Silk Road: What has this meant for online drug trading? *Addiction*, *109*, 517-518.

Van Hout, M. C., & Bingham, T (2013). 'Surfing the Silk Road': A study of users' experiences. *International Journal of Drug Policy*, *24*, 524-529.

Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy*, *25*, 183-189.

Wehinger, F. (2011). *The dark net: Self-regulation dynamics of illegal online markets for identities and related services*. Paper presented at the European Intelligence and Security Informatics Conference, Athens, Greece. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6061236

Williams, P., & Copes, H. (2005). "How edge are you?" Constructing authentic identities and subcultural boundaries in a straight edge internet forum. *Symbolic Interaction*, *28*, 67-89.

Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology*, *2*, 407-427.

Blog and Forum Posts

Agora Marketplace Forums. (2014, May 9). Re: *The Scurvy Crew—Reviews and AWESOMENESS! Home of the finest hash, weed n' opium, Agora*. Unavailable online due to closure.

DeepDotWeb. (2013a, December 6th). *Black market reloaded hacked—Around 200.000$ stolen*. Retrieved from http://www.deepdotweb.com/2013/12/06/bmr-hacked-around-200000-stolen/

DeepDotWeb. (2013b, December 14). *TorMarket hacked—Database leaked by . . . Dread pirate Roberts*. Retrieved from http://www.deepdotweb.com/2013/12/14/tormarket-hacked-database-leaked-by-dread-pirate-roberts/

DeepDotWeb. (2013c, December 13). "*So what's going on with all these DDOS attacks?"* Retrieved from http://www.deepdotweb.com/2013/12/13/so-whats-going-on-with-all-these-ddos-attacks/

DeepDotWeb. (2014a, March 20). *Pandora marketplace hacked: Losing 250.000$ in BTC*. Retrieved from http://www.deepdotweb.com/2014/03/20/pandora-hacked-losing-50-btc/

DeepDotWeb. (2014b, August 25). *Cannabis Road hacked: $100.000 (~200 Bitcoins) gone*. Retrieved from http://www.deepdotweb.com/2014/08/25/cannabis-road-hacked-100000-in-btc-gone/

DeepDotWeb. (2014c, February 13). *Silk Road 2.0 hacked, all bitcoins stolen—$2.7 million*. Retrieved from http://www.deepdotweb.com/2014/02/13/silk-road-2-hacked-bitcoins-stolen-unknown-amount/

DeepDotWeb. (2014d, May 21). *A scammer's remorse*. Retrieved from http://www.deepdotweb.co/2014/05/21/scammers-remorse/

DeepDotWeb. (2014e, August 1). *Outlaw market down—Possibly compromised by competitors*. Retrieved from http://www.deepdotweb.com/2014/08/01/outlaw-market-down-possibily-compromised/

DeepDotWeb. (2014f, March 10). *What to do while your favorite market is under attack*. Retrieved from http://www.deepdotweb.com/2014/03/10/what-to-do-while-your-favorite-market-is-under-attack-agora/

DeepDotWeb. (2014g, January 29). *Cantina marketplace PWND: Admin password was: "Password1"?!'* Retrieved from http://www.deepdotweb.com/2014/01/29/cantina-marketplace-pwnd-admin-password-was-password1/

DeepDotWeb. (2014h, February 9). *Another two bites the dust (Black Goblin & Cannabis Road)*. Retrieved from http://www.deepdotweb.com/2014/02/09/another-two-bites-the-dust-black-goblin-marketplace-cannabisroad/

DeepDotWeb. (2015a. March 6). *Tutorial: How to buy from Agora marketplace*? Retrieved from https://www.deepdotweb.com/2015/03/06/tutorial-how-to-buy-from-agora-marketplace/

DeepDotWeb. (2015b, March 18). *Evolution marketplace exit scam: Biggest exist scam ever?* Retrieved from https://www.deepdotweb.com/2015/03/18/evolution-marketplace-exit-scam-biggest-exist-scam-ever/

Reddit. (2014a, November 20). *Darknet market scams, a revised list, u/darknetsolutions*. Retrieved from http://www.reddit.com/r/DarkNetMarkets/comments/1uz9y4/darknet_market_scams_a_revised_list/

Reddit. (2014b, May 2). *PSA: Using your street smarts on the deep web*. Retrieved from http://www.reddit.com/r/DarkNetMarkets/comments/24jvi1/psa_using_your_street_smarts_on_the_deep_web/

Reddit. (2015). *Postal systems and drops*. Retrieved from https://www.reddit.com/r/DarkNetMarketsNoobs/wiki/postsysanddrops

Tor Project. (2013). *Hidden services need some love, asn, April 22nd 2013*. Retrieved from https://blog.torproject.org/blog/hidden-services-need-some-love

Tor Project. (2014, January 24). *New Tor denial of service attacks and defenses*. Retrieved from https://blog.torproject.org/blog/new-tor-denial-service-attacks-and-defenses

Author Biographies

Kim Moeller, PhD, is an associate professor and study leader at the Department of Criminology, Aalborg University, Denmark. His research has recently been published in the *Journal of Research in Crime and Delinquency, Justice Quarterly*, and *Journal of Criminal Justice*.

Rasmus Munksgaard has an MsC in sociology from the University of Copenhagen and is currently a PhD student at École de Criminologié at the Université de Montréal. His current work explores behavioral and social aspects of trust in the context of cryptomarkets.

Jakob Demant holds a PhD in sociology and is an associate professor at the Department of Sociology, University of Copenhagen, Denmark. He has published more than 50 journal articles on the subject of crime, alcohol, drugs, and cryptomarkets.