“We must work together for the good of all”: An examination of conflict management on two popular cryptomarkets

Jeremy Cheung

Abstract. For nearly ten years, illicit markets have taken advantage of the anonymity and convenience afforded by the dark web. Despite its benefits, however, this anonymity has also resulted in difficulties establishing trust and managing conflict on cryptomarkets. A number of common features have been implemented to serve this function. This study was conducted to contribute to the growing literature on conflict management in cryptomarkets through a thematic analysis of publicly available content from two popular cryptomarkets. Of particular interest is whether conflict management has changed following the closure of many popular cryptomarkets and how conflicts are managed differently in relation to unique types of transaction or delivery offered by the marketplaces under study. Findings indicate that, rather than evolving to become different from those marketplaces that have been shut down, the two marketplaces under study have slowly changed to become more like them, based on suggestions from users. Implications for law enforcement are discussed.

Introduction

The proliferation of the Internet has led to many criminal enterprises transitioning online to the dark web: an area of the Internet offering near-complete anonymity to its users. However, this anonymity has proven to be a double-edged sword, changing the nature of trust integral to co-offending partnerships and networks and enabling effortless infiltration by law enforcement agents (Moeller, Munksgaard, & Demant, 2017). Consequently, new means of managing conflict and establishing trust have had to evolve alongside this new convenient platform for the trade of illicit goods and services. These new means of managing conflict have in turn had to adapt in response to the disruption and even shutting-down of marketplaces by law enforcement as well as fraudulent administrators (van Buskirk et al., 2017).

The purpose of this study is to undertake a phenomenological thematic analysis of conflict management in two popular dark web marketplaces: Tochka Free Market (TFM) and Wall Street Market (WSM). The central question is how do users – which include vendors, buyers, and administrators – manage conflicts among themselves while participating in dark web cryptomarkets? In answering this question, I contextualize my findings in broader literature on social control and conflict management in both online and offline illicit markets and discuss implications for cryptomarket users as well as law enforcement. Of interest is also whether the management of marketplace conflict has changed in light of successful law enforcement operations and fraudulent practices by marketplace administrators.

What are Cryptomarkets?

Cryptomarkets are Internet-based platforms that use encryption software to protect users' identities and facilitate the exchange of (often illicit) goods and services. They can only be accessed using the Tor browser, which is freely available to the public and uses anonymizing software to route an individual's Internet activity through various nodes with layers of encryption that mask their IP address to make their activities untraceable. Both buyers and sellers log into cryptomarket sites anonymously through the Tor network (Chertoff, 2017; Dolliver & Kennedy, 2016; Martin, 2014). Once a marketplace has been accessed, goods and services can only be purchased using cryptocurrencies such as Bitcoin or Zerocoin, which function similarly to regular, non-virtual currencies and are purchased through legitimate vendors to avoid counterfeiting (Chertoff, 2017; Martin, 2014). The difference is that each transaction involving these currencies is encrypted so it is difficult, if not impossible, to link payments to individuals (Aldridge & Askew, 2017; Martin, 2014). The fact that transactions are made online also makes it harder to link the activities of buyers to sellers, compared to offline markets, where proximity is a necessary condition of the trade (Martin, 2014). Rather than arranging a transaction online and meeting subsequently in person, licit postal services are traditionally used, although dead drops have grown in popularity recently as well. Thus, rather than two criminals crossing paths for a criminal transaction, the interaction is spread out geographically and merged with licit activities (Aldridge & Askew, 2017). Finally, encrypted messaging software such as PGP (pretty good privacy) or Privnote is also used to secure two-way communications between users as an added safeguard (Aldridge & Askew, 2017).

In addition to the lowered risk of detection, cryptomarkets offer a number of other appealing features. First, the risk of physical violence to market participants is circumvented due to their anonymity and remoteness from one another. Especially in the drug trade – where a substantial amount of cryptomarket activity occurs – there tends to be a continuum of real and perceived risk of violence (Morselli et al., 2017). The second appeal is accessibility. Sellers constrained by physical boundaries in offline markets, especially those in countries with a small consumer base, now have access to booming international markets. Similarly, buyers with little access to illicit goods and services can now pick and choose from an array of the finest products in the world. The only requirement is an Internet connection, Tor browser, and cryptocurrencies, all of which are publicly available and accessible through ubiquitous technologies (Dolliver & Kennedy, 2016). Lastly, and in complement of their accessibility, cryptomarkets are very user-friendly, modeled after popular online shopping platforms such as eBay and Amazon. Prior to making a purchase, prospective buyers can browse various listings, filter and sort their search results by categories and subcategories of goods and services, and inspect profiles of vendors who each have ratings from past buyers describing the standard of products, customer service, and timeliness of delivery (Martin, 2014). Whereas individuals looking to purchase illicit goods and services offline may be unsure of how to approach sellers or check their reliability, users of cryptomarkets may find the friendly and familiar interface welcoming and easily navigable.

The Importance of Conflict Management

Conflict management in cryptomarkets is worth studying because of its importance to the perceived legitimacy and proper functioning of these marketplaces. Despite the numerous benefits associated with cryptomarket use, the reality remains that any form of business, illicit or otherwise, requires trust and some mechanism of accountability/oversight to prevent and mitigate conflict and guarantee a successful transaction. In legitimate business dealings, there may be several avenues of legal recourse for bad faith or fraudulence (e.g., calling the police or invoking a legally enforceable clause in a contract). Even in offline illicit markets, where participants must work against the state and without its benefits, there are alternative means of establishing trust and forms of social control (e.g., the use of violence). The initial requirement of proximity in many cases also creates a subsequent risk of later being tracked down by disgruntled business partners, which serves as a deterrent to wrongdoing in itself (Morselli et al., 2017).

Cryptomarkets, however, are characterized by anonymity and isolation from all parties involved. This is compounded by a risk that any party in a transaction is a law enforcement agent. Under these conditions of uncertainty in the absence of means to establish trust, cryptomarkets may take on the properties of a “lemon” market, where there is an unwillingness for buyers to pay asking price or full price for a commodity (Yip, Webber, & Shadbolt, 2013). This, in turn, results in low market participation. As such, new methods of establishing trust by preventing and resolving conflict are needed (Yip et al., 2013).

Four standard mechanisms of accountability and conflict management have emerged in cryptomarkets. The first is an escrow system, which discourages vendors from scamming buyers. Once a buyer has found a listing they wish to purchase, they surrender the appropriate funds to an escrow service hosted by marketplace administrators, where money is withheld from the vendor until the buyer has expressed that they have received the product as promised or the requested service has been carried out (Tzanetakis, Kamphausen, Werse, & von Laufenberg, 2016). The second mechanism is a vendor feedback system. Upon receipt of the good or service, a buyer can rate the vendor based on their satisfaction and may provide comments to guide the decisions of other prospective buyers. Complementing the escrow and vendor feedback systems is a third mechanism of formal arbitration by staff or administrators. If a buyer is dissatisfied with what they have paid for, a vendor is unhappy with a review, these matters can be dealt with privately with the help of the staff. Whereas the first two mechanisms protect buyers from vendors, this system allows vendors to raise disputes against buyers. The fourth mechanism of conflict management is a publicly available forum for all market users, who can share experiences about other users, operational security, law enforcement tactics, and other content. Whereas the first three mechanisms are private means of conflict management and protect buyers and vendors only from each other, these forums can be used to manage conflicts involving administrators themselves (Morselli et al., 2017). For example, exit scams occur when marketplace administrators empty funds held in escrow into their own accounts and flee.

Data & Methods

This study is a phenomenological thematic analysis, exploring conflict management among users of dark web cryptomarkets through "publicly" available information on these marketplaces. Conflict management is defined as the ways in which marketplace-related conflicts and victimizations are prevented, as well as how grievances are communicated and subsequently addressed by cryptomarket users. This is replication of Morselli et al.'s (2017) prior research examining conflict management in ten popular marketplaces to uncover and explore self-regulating mechanisms designed to address disputes arising from transactions and how violence or the threat thereof compared to other means of settling conflict in the milieu of cyberspace and anonymity. I deviate from Morselli et al.'s (2017) research design by additionally sampling vendor profiles and using a purposive data collection method described below.

Data Sources and Collection

The cases studied are individual marketplaces, TFM and WSM, chosen for their popularity, purported uniqueness, and wide range of goods and services offered. At the time of collection, WSM and TFM were ranked as the second and third most popular cryptomarkets, respectively (DeepDotWeb, 2019). The success and popularity of these marketplaces may indicate effective systems of conflict management, making them suitable for answering the research question. That both cryptomarkets offer a range of goods and services rather than specializing in a certain commodity is desirable because if conflict management differs based on the types of goods and services sold, studying TFM and WSM could yield conflict management data that is representative of these different types of marketplaces.

The content was sampled from three publicly accessible domains in each cryptomarket: (1) the terms of use or codes of conduct; (2) marketplace forums; and (3) vendor profiles and reviews. The terms of use for both TFM and WSM were coded in their entirety since they were short and each clause therein uniquely governed behaviour. Forum threads and posts were selected purposively to achieve a representative sample of the range of sources of conflict and methods of conflict resolution and prevention in each marketplace. If threads were plainly unrelated to conflict or posts reflected already saturated codes or themes, they were not included. This purposive strategy should allow an observation of a potentially more varied and sophisticated landscape of conflict management and market regulation than limiting collection to an arbitrary date range. Posts were considered relevant to conflict management if they related to wrongdoing against another user or expression of concern (or praise) over a transaction, interaction, or some other aspect/feature of the marketplace and its management.

Over 1500 forum posts were read under general topics related to scamming, law enforcement, support, operational security, and marketplace policies, and 897 were ultimately collected and processed for later coding. Lastly, vendor profiles were selected purposively to achieve a sample representative of each class of good/service offered in the marketplace and of each type of transaction (e.g., escrow, direct deposit) and delivery (e.g., mail, dead drop). 30 vendor profiles across both marketplaces were viewed and 12 were ultimately processed for later coding. Since all members of the public are free to make an account to access TFM and

WSM, the content is considered to be in the public domain. I did not interact with any marketplace users and all usernames have been disassociated from their content, while all raw data has been encrypted using VeraCrypt. These facts and precautions combine to make this research exempt from ethics review according to both the TCPS-2 and SFU's institutional research ethics policy.

Data Exploration and Analysis

Coding took place both deductively and inductively. I began deductively with a small set of codes derived from Morselli et al.'s (2017) analysis of conflict management from ten cryptomarket forums. These codes referred to *sources* of conflict and conflict *resolution* strategies. More codes were inductively added where Morselli et al.'s (2017) did not seem to accurately describe data. Content was also inductively coded for conflict *prevention* strategies. This process could also be defined in terms of manifest and latent coding, which refers to the more mechanical or superficial units of meaning and the deeper underlying meaning, respectively (Hesse-Biber, 2017). Manifest coding involved recording the source of data, types of users generating the content or who is being referred to in the content, and if applicable, the type of transaction or delivery associated with the comments. Latent coding was also done simultaneously, indicating the type of determinant/source of conflict, conflict resolution strategy, or conflict prevention strategy. After the initial round of coding, the content under each code was analyzed and more specific codes were inductively nested under broader ones. The result was 98 codes that could be categorized as sources of conflict, conflict resolution strategies and conflict prevention strategies, as well as types of transactions, types of delivery, and general characteristics regarding risk, trust, and uncertainty on cryptomarkets.

Table 1. Primary codes and categories

Sources of conflict	Conflict management strategies	
	Conflict resolution strategies	Conflict prevention strategies
Scamming*	Active	Forum-based instructions and suggestions
Bad market management*	Ostracism*	Member-checking
Law enforcement activities*	Third-party intervention*	Policymaking
Unfair competitive practices*	Call for help	User-shared advice
Transaction failures*	Leaving a bad review	Suggestions to staff
Social interactions*	Threats*	Vendor profiles
Technical difficulties	Official inquiry	Operational security
Technical rule violations	Negotiation*	Reputation management
Bad advice	Self-defence	Dealing with stupid customers
Innocuous stupidity	Passive	Marketplace rules / codes of conduct
Unprofessionalism	Avoidance*	Forbidden acts and activities
Risk of physical danger	Tolerance*	Forbidden goods and services
	Shaming	Dispute resolution policy
	Victim blaming	User responsibilities
	Empty retaliation	
	Admission of guilt	
	Apologizing	

*Deductive codes from Morselli et al. (2017)

Findings

Conflict prevention strategies were seen across each source of data in both TFM and WSM, whereas methods of conflict resolution strategies appear to be restricted to the vendor feedback system and marketplace forums. Although the codes adopted from Morselli et al.'s (2017) study could be used to accurately describe the majority of sources of conflict and conflict resolution strategies, Table 1 shows six additional sources of conflict and nine additional conflict resolution strategies were found for a total of 12 sources and 15 resolution strategies. Lastly, 14 conflict prevention strategies were also found. Only the most common and notable codes and categories are discussed below. Less important or interesting ones are subsumed under discussions of other codes.

Sources of Conflict

Scams. By far the most common source of conflict in both TFM and WSM was scamming. This term refers generally to some fraudulent exchange and was applied to all types of users. Even conflicts arising from many of the other sources of conflict found were often labeled by users as scams. For example, vendors openly accused buyers of blackmailing them by falsely leaving negative reviews and notifying the vendors that they will not change the review until more product is delivered or payment is reversed. In a system where a vendor's reputation is everything, this type of scam can be very damaging. Similarly, concerns about exit scams by marketplace staff were common:

> **Vendor:** …from what I've been hearing seems like the owner is planning a exit scam. He's been banning vendors and stealing money from them on a daily basis. Don't really know if this is him directly or somebody else, but I would refrain from opening a vendor account there.

The more "traditional" scam, however, involved a vendor withholding product from a buyer. This happened despite the existence and encouraged use of escrow services in both TFM and WSM because of the transaction types used. Although off-market deals are banned explicitly by the terms of use for both marketplaces, vendors appeared to frequently request that buyers interact with them off-market via encrypted messaging services such as Wickr, and/or send them money directly off-market rather than depositing the money in escrow. The "first" option available only on WSM interestingly mimics the effect of off-market deals since payment is deposited directly into vendors' virtual wallets.

> This is how i was lured offsite saying tochka was doing exitscams that how [vendor] got me to use wickr i knew i was taking a chance what a fool i was..yeap. scammed

Another user was the victim of a far more elaborate plan, involving the use of fake shipment tracking sites and continuously solicited payments:

> I recently paid @mattholland for an order over the Marketplace, and he took the convo to Wickr – started simple enough, extra $ for expedited shipping. Okay. Then the package gets stuck in customs. He send me a shipping agency called skyfastshipping.com (and http address d'oh) and ask for more and more

> payments to get what I ordered through customs. […] I stupidly decided to just sent him what I had in my wallet of cash via bitcoin atm and he says that the fees taken out reduced it by nearly $50... he tells me that the police are going to find me, I'm in panic mode (like an idiot, I know, I know) so the next morning I withdraw and deposit $100 […] to "get it through customs", and he told me to resend because the transaction cancelled. He reminds me that the customs fee is refundable too once it's delivered LOL.

Although a discourse has been developing on forums warning users of this exact type of scam, there were numerous reports of these types of victimizations, typically by inexperienced buyers.

The presence of a "finalize early" (FE) option in both marketplaces was also used to circumvent the escrow system. Once a buyer selects this option, the funds are immediately released to the vendor from escrow. Thus, although the escrow system is not avoided completely, its effectiveness as a method for establishing accountability is diminished. This effectiveness arguably hinges on funds being released to vendors no earlier than the time a buyer receives their goods as promised.

> **Buyer 1:** I was an idiot and FE'd when he asked me to "in order to get the tracking code." It's been 2 weeks since FE and no response other then It will shipped soon immediately after Release. I hope he didn't get anyone else, Stay Away
>
> **Buyer 2:** NEVER EVER FE with anyone. I don't care how much buying history yall have. Always stick with escrow.

Bad market management. It is significant that conflict management was such a common source of conflict because the marketplace itself is meant to be part of the solution to conflict. However, it is precisely for this reason that vendors and buyers publicly launched grievances against market staff: they were believed to not be doing their jobs properly. Allegations of other conflicts were often followed by complaints against management for allowing those conflicts to occur or not taking desired action. In the following example, a vendor is frustrated by the amount of support for buyers, but not sellers in the midst of a rise in buyer-perpetrated scams:

> **Vendor:** This market is good but Admin, it needs to get better. All focus are on sellers as scammers whereas some scammers now pose as buyers to scam sellers. I witness how […] [w]hen this buyer noticed [their] item close to deliver, a report was made by the buyer and the transaction was frozen. The buyer received the packaged and deny receiving the package so the order was cancelled. […] My question now is , how are the sellers protected as well?

These were typical allegations of platform mismanagement, where users were aggrieved by perceived inadequacies in the ways staff were carrying out their duties. However, as shown earlier, marketplace scams such as exit scams were also a common form of bad market management, in addition to other allegations which revolved around conspiracy and supporting non-staff scammers:

> **Buyer:** [Vendor] is a scammer he is selling and advertising a cashout guide that he knows does not work...i made a post about it in fraud […] and mods deleted the post! They are censoring any negative feedback about him.

At the same time, members were also quick to express support and gratitude to the marketplace and its staff and defend them when they felt an allegation was inappropriate or unjustified. For example:

> **Buyer**: u suck as a MOD, deleting my post, your a joke with no compassion for others, i hope your luck goes down a drain
>
> **Community Manager**: Sir, you did a post on the wrong place: Don't post off-topic posts here, we have a off-topic section and a funny & jokes for this. Any off-topic will be deleted without any warning. You did a post on the wrong place, there's the correct place for this.
>
> **Vendor 1**: Haha, [Community Manager] sucks as a mod... He's kinda the best there is.
>
> **Vendor 2**: He is a community manager, and a damn good one!
>
> **Community Manager**: Thanks guys.

In this example, two vendors come to the defence of a WSM community manager who was verbally assaulted by another member, apparently upset over having their joke deleted. The post was originally placed in a thread under a topic called “LE [law enforcement] Watch & Arrest Reports,” where users kept each other apprised of law enforcement activity on other markets, arrests of existing vendors, and operational security techniques. The community manager’s actions in deleting trivial matters from threads under this topic reflect the importance that all users give to safety and detection avoidance.

Law enforcement activities. It appeared that inadvertently doing business with law enforcement was seen as far more undesirable than being scammed. If a user was scammed, they could continue to do business. The losses are purely financial. However, the potential losses are far greater when detected by law enforcement. A common fear for buyers is that they are purchasing from vendors who have been arrested and whose accounts are now being operated by law enforcement. As mentioned above, WSM has an entire topic on their forum dedicated to law enforcement activities titled “LE Watch & Arrest Reports.” Here, entire news articles about the apprehension of cryptomarket users and other relevant subjects are pasted into threads for educational purposes, as is content about how to avoid detection from law enforcement.

Unfair competitive practices. Unfair competitive practices are acts of sabotage that most frequently involved covert acts of using buyer accounts to purchase from a competitor and leave negative feedback using the review system on a vendor’s profile or on public forum threads. The following post from TFM shows a vendor replying to a post identifying them as a scammer:

> I'm 100% sure you are a team member of those several motherfuckers trying to destroy my good reputation but trust me that's not gonna work for you cos my profile can never be destroyed no matter what.

In contrast to the buyer-scams described above, this does not involve blackmail; rather, it involves the use of slanderous comments to tarnish a vendor's reputation. Similarly, there are also allegations on forums of vendors paying buyers to leave negative reviews:

> **Buyer:** [buyer] is just a big fool, jobless idiot who doesn't have anything to do. you thing i don't know what you do in this market ? when you get paid to fake reviews for vendors you are such a stupid fool

These unfair competitive practices are detrimental to the overall functioning of a marketplace because they delegitimize systems of conflict management such as public forums or the vendor review system, thereby contributing to the lemonization of a market.

Technical difficulties. Technical difficulties, despite being innocuous compared to the risks associated with scams and law enforcement intervention, frequently invoked panic especially among new buyers. There is always fear when encountering such difficulties that one is being scammed and that the technical difficulties are in fact evidence of deliberate misconduct. In other cases, however, technical difficulties can be barriers to efforts to resolve conflict or ascertain the likelihood that one has been scammed.

> **Buyer 1:** I am trying to dispute an order, whenever i try to do that i get an error message saying " 404 - Page Not Found ". Could you please help me resolving this? This is my first time trying to dispute an order
>
> **Buyer 2:** I'm having the exact same problem, and my vendor is 100% scamming as they provided me with a tracking number for a fake courier website swiftexpressmail.com. I keep getting the same error 404 page not found. Any help on this ADMINS?

In this example, two buyers trying to open a dispute are unable to do so. Given the importance of this system of conflict management, such technical difficulties are important sources of conflict.

Technical rule violations. Technical rule violations are innocuous rule transgressions, usually by users who have not taken the time to learn such rules and do not know any better. However, more experienced users are also guilty of this, especially vendors:

> **Buyer:** Hello I agree completely with many sellers do not respect the rules of this store and that can only be solved with the expulsion from the store of those sellers and it is the job of everyone and especially the administrators of this website I have deposited an order 4 days ago and the seller does not answer. We must work together for the good of all.

In fact, numerous reputable vendors in their profiles have listed their Wickr or Jabber handles and encourage buyers to contact them offsite for quicker service. These rules or behavioural guidelines are considered sacred by many users though, since they are the foundation of conflict prevention on cryptomarkets. A person who follows these rules should not be able to

scam users and should also be able to avoid victimization themselves. Thus, there is a fear that those who offend the rules are scammers or law enforcement agents, regardless of whether they are actually transgressing the rules in bad faith. This is exemplified in the following quote:

> **Member:** stop doing things that LE does and your name won't be in this section, and no one will be asking you to explain your activities. There is too much LE freely going on all DNMS, opening up accounts and probing vendors and other buyers, collecting entirely too much intormation, it needs to be somewhat regulated as to what kinds of questions are [asking] vendors and other buyers. please be careful everyone […] You should see some of the budget's countries like Canada and Australia have for Cyber Operations...

Conflict Resolution Strategies

Active conflict resolution strategies. Just as Morselli et al. (2017) found, ostracism was by far the most common conflict resolution strategy observed. However, this could also be an artefact of forums being an informal conflict resolution mechanism used by non-staff users of cryptomarkets, and that the data excludes private communications between staff and other users. Ostracism occurs when a victim of a scam or any other offence identifies their wrongdoer on a public forum:

> **Buyer:** i can confirm @[vendor 1] and @[vendor 2] are big time scammers, please avoid these individuals and under no circumstances do any business with them!!!

This quote shows a typical example of ostracism, where a wrongdoer is named and others are warned to stay away from them. If the wrongdoer is a vendor, this could also involve a buyer leaving negative feedback on their profiles. For example, upon being scammed on TFM, a buyer left the following review:

> **Buyer:** AVOID AT ALL COSTS! I should have read the bad reviews, but took a chance. I ordered a scanned US passport, and asked for it to be of a caucasian woman born in the late 80s or 90s. Seller agreed, but upon delivery it was of a Thai woman born 1964. [Rating:] 1/5

For both TFM and WSM, the forum topics with by far the most activity were those related to ostracizing scammers. Interestingly, some members became highly active on these threads, providing a sort of vigilantism and taking it upon themselves to conduct research on the trustworthiness of cryptomarket members. One buyer, after being scammed, went on to ostracize over one hundred fake buyers and illegitimate sellers, concluding in some cases that certain accounts were operated by the same person based on shared encryption keys and linguistic comparisons of reviews by different users. Ostracism is, at least in theory, very effective. If a buyer was publicly ostracized, vendors may be unwilling to sell them anything; if vendors were ostracized, they may lose business. In both cases, the vendor or buyer is also at risk of being sanctioned by the marketplace administrators. However, since it is so easy to create accounts, it is entirely possible for banned users to simply come back and pick up where they left off.

Third-party intervention may involve formal intervention by a staff member or more informal intervention by another member. Types of marketplace intervention can range in severity from being instructed to open a support ticket to the banning of users (Morselli et al., 2017). On TFM, a common observation on scam-related threads was descriptions of wrongdoing by users followed by a short reply of "Banned" by an administrator, indicating that a transgressor had been dealt with swiftly. Although content from support tickets was not publicly available, some users did describe successful calls for help:

> **Buyer:** Hey, New to market. Attempted to make first transaction. As soon as I funded the escrow account vendor removed all items from his sale list and asked that I FE my order ASAP so that he could ship […] How do I cancel? What to do from here
>
> **Buyer:** Quick update - Staff cancelled order almost immediatetly as I explained the situation. Just waiting for the funds to reach my account. Will update when it does. In any event. I will definetly try another vendor on this market. Staff is great.

Finally, third-party intervention commonly involved asking cryptomarket staff to implement changes. These will be discussed more in relation to conflict prevention strategies.

Threats, although relatively uncommon, were made against all types of users to intimidate wrongdoers. While some threats were empty, others involved compromising a user's anonymity or use of physical violence. When made against the marketplace, threats often included allusions to shutting down its operations and/or involvement of law enforcement agents. For example, a disgruntled banned user on WSM wrote:

> [administrator 1] and [administrator 2] fuck both of you. why the fuck did u ban me. Mark me i will take WSM down, i promise. I will frame you and u will be busted. We told Alphabay the same thing and now they are down. WE ARE ANONYNOUS WE ARE LEGION WE DO NOT FORGIVE

The most interesting and unique form of active conflict resolution was found on WSM, when a non-staff member used the forum to open an "official" inquiry against a vendor who had received numerous allegations of being a scammer:

> **Buyer:** 1. [vendor] Did you or did you not ask a wall street user for their personal bitcoin address so you could "Send them a tip?" Just a yes or no will suffice … 2. [vendor] Do you or do you not write reviews for vendors on here and try to find out as much about them as you possibly can by trying to engage them in a variety of subjects? Do you ask them about personal subjects? … 3. [vendor] Can you explain what is your real motivation for being on this forum more than any other users and having more posts than any other vendor or user basically? […] I have every right to ask you these questions, and am doing so in a professional and respectful manner so please provide direct answers.

This is not the same as ostracism since the vendor was given an opportunity to defend himself. Many users attended the inquiry (i.e., viewed the thread), posting support for the buyer who

initiated it and demanding justice. The vendor eventually replied to the thread, but was ultimately banned by marketplace administrators. This is an exemplary demonstration of the level of community observed on either marketplace.

Passive conflict resolution strategies. Tolerance as a conflict resolution strategy involves no direct response to the wrongdoer. The use of tolerance appears to be largely due to the anonymity of cryptomarkets and limited available recourse, especially for those who were scammed off-market. Once some form of victimization occurs, it can be very difficult to resolve the conflict, leading to apathy. For example:

> **Buyer:** this a little ridiculous honestly. I am sorry you had a bad experience with one vendor, but that doesn't mean you have to go on a witch hunt.

Another buyer interjecting into another user's call for third-party intervention said:

> **Buyer:** Admin you should investigate and not just take any actions[.] If he contracted him off market do not blame the vendor because buyers are warned but they still go for off market deals

In fact, there appears to be a common theme of "acceptable risk." That is, users acknowledge that certain risks are associated with doing business on the dark web and expect that some losses are inevitable. Vendors routinely expect buyers to take risks:

> **Vendor:** NO REFUNDS/REPLACEMENTS FOR CUSTOMERS WHO DO NOT UNDERSTAND CARDING IS A GAMBLE AND NOT EVERY CARD IS A HIT. JUST BECAUSE YOUR METHOD DIDN'T WORK DOESN'T MEAN THE CARD WASN'T LIVE WHEN SENT. MY JOB IS TO SEND LIVE CARDS. YOUR JOB IS TO CARD AND I AM NOT RESPONSIBLE FOR YOUR METHODS WORKING OR NOT ONCE I SEND A LIVE CARD.

The above quote is part of a disclaimer from a vendor selling credit card information in bulk, who reminds buyers that it is perfectly normal and not dispute-worthy to obtain bad product. Avoidance is similar in that no action is taken against a wrongdoer. However, rather than pure inaction, a victim may decide to change marketplaces and even warn others to do the same:

> **Buyer:** Both vendors asked me to FE before "going with my order" What a waste of time, I thought this site looked good but just a bunch of scammers. Sucks, will be taking my money elsewhere.

Shaming and victim-blaming were common responses to victimization, especially where a user was acting outside the rules designed to protect them. This way of addressing conflict is considered passive because it does not involve the resolution of conflict and involves a recommendation of inaction. Shaming responses can be either sympathetic or negative as the example below shows:

> **Buyer:** Sorry it cost so much for you to learn this lesson, but yeah, you can't allow yourself to get roped in by "too good to be true" shit. When I first got into dnms I was stupid enough to use links on The Hidden Wiki, and fell for one of those bullshit "Send us 1 btc and get double your money through paypal" scams.

> **Vendor:** You actually fell for these scams? Sorry to hear that. It's so obvious that it's all a scam. The few people who fall prey to this is what keeps it alive. WSM should do something about this. But they're not going to. So instead people should use common sense.

Even staff were observed blaming victims for their own misfortune:

> **Community Manager:** Funny, you do an offmarket deal and then want us to become darknet cops. Sir, we work hard to provide escrow. Scammers will try to scam and you should pay attention and never fall on their tricks.

In this case, buyers complained to staff calling for help after conducting a deal off-market.

Conflict Prevention

Marketplace rules and codes of conduct. Marketplace rules, or "rules of engagement" as termed by Morselli et al. (2017), are terms of use that each user must follow. Both TFM and WSM set out the various permissible delivery and transaction types with both forbidding off-market business. Interestingly, both cryptomarkets also attached warnings to transaction options other than escrow, stating unequivocally that other methods were more likely to result in losses. Despite WSM being known for the convenience of their First (i.e., direct deposit) option (DeepDotWeb), they have made it only available to vendors with the "trusted" status and announced that it is the most unsafe trading option. TFM and WSM also include conflict resolution policies and lists of responsibilities for each type of user, as well as forbidden acts and activities, such as off-market deals or sale of child pornography. TFM goes one step further, even requiring all vendors to sign a vendorship agreement with the appearance of a legally-binding contract.

Forum-based instructions and suggestions. In addition to being an extremely valuable platform for responding to conflict, cryptomarket forums are also important for its prevention. For example, forums can be used by buyers to check the trustworthiness of vendors prior to a purchase. On the same threads used by scam victims to ostracize wrongdoers, users would proactively inquire about a seller from whom they were thinking of buying:

> **Buyer:** is @[vendor] a scammer? pls i need to know before i purchase from him, and can he truly he ship to anywhere in the world

Similarly, buyers would also ask about the delivery services, tracking websites, and/or money services used by vendors to be extra sure of their legitimacy.

Members also frequently made suggestions to staff on ways the marketplace could improve. Vendors being blackmailed by buyers suggested a buyer-rating system be implemented. The popular "LE Watch & Arrest Reports" topic on WSM originated because of a suggestion from a member:

> **Vendor:** Agora Reloaded had an Arrest Reports Section. This was actually helpful info. Something like an LE Watch/Arrest Reports Section would be great similar to scamwatch but if a user is doing anything that is LE suspicious like the following things it should be reported and dealt with.

Interestingly, the public forums were not only used to effect conflict prevention by buyers or vendors. Marketplace staff and administrators also frequently used these marketplaces to reactively create policies:

> **Moderator:** These rules are being posted and all rules must be read and understoo[d] before posting, there will not be any reminders or warning to these rules. If any forum member is caught breaking these rules you can be banned, thanks in advance. These rules are here to make the forum a safe [a]nd productive part of the WSM community.

Vendor profiles. Vendor profiles are also a very important for conflict management, beyond being attached to a feedback system where prospective buyers can determine their quality of service and trustworthiness. Vendors often take precautionary measures in their introductory messages within their profiles, to protect themselves as well as their buyers. To ensure protection of their reputations, vendors typically provide disclaimers to lower expectations of a successful transaction/delivery while also providing good customer service, as shown above. Similarly, vendors may write contingencies into the conditions of business to avoid dissatisfaction from becoming public. For example,

> **Vendor:** Positive feedback is much appreciated! Please don't give negative feedback if there is a dispute. I understand there is always a risk and I will always try to find the fairest solution for both parties. Leaving negative feedback without respectful communication beforehand means no reshipment and no further business.

To ensure customers are protected and to avoid detection, "stealth" measures are employed to disguise packages:

> With packaging for your orders , you have no fear as we use scanner proof nylons to wrap up your product then later on vacuum seal the products double for marijuana orders to avoid that smell and then disguise most at times by shipping in a playstation 4 Game console, This is just one of our shipping techniques as we have many others in store to ensure that you get your order without any custom interception , no mater your location.

Discussion & Conclusion

This paper follows the lead of Morselli et al. (2017) and other authors (e.g., Moeller et al., 2017) who have studied the management of conflict in cryptomarkets. All responses to conflict are consistent with the literature on conflict management and no new strategies/mechanisms for responding to conflict were observed. The primary conclusion is therefore that all forms of conflict management examined in extant literature (discussed above) are still at least perceived to be the most effective: existing methods of conflict management are flexible and appealing to users, such that new features and innovations such as TFM's dead drops are seldom offered or discussed and WSM's "First" (direct deposit) option is openly discouraged by all users including management. Many conflicts observed in TFM and WSM could have been avoided by proper use of the escrow system and simply following the rules that marketplace administrators put in

place to protect its users. One reason for the observation of these common features may be the critical discourse that takes place in forums, where users from other markets share experiences and knowledge that made those other markets successful. Perhaps this is also the reason TFM and WSM have become so popular in the first place; they may have been more receptive to these suggestions than less popular marketplaces.

However, the numerous forms of conflict prevention/resolution described cannot fix all vulnerabilities. A major overarching source of conflict is human error stemming from inexperience and naivety. This has implications for law enforcement, since inexperienced and naïve users are easy targets. The volume of scams documented resulting from off-market deals, for example, means that it may be easy to persuade new buyers to conduct business away from the relative safety and anonymity of the dark web. After buyers are identified, their accounts can be commandeered and used to create conflict within a marketplace (Yip et al., 2013). Furthermore, the diversity of conflict that exists in cryptomarkets spoils law enforcement users with plausible deniability. For example, negative reviews or allegations of scamming made against a vendor account controlled by law enforcement can be neutralized by informing other users that the package was lost in transit or that the allegation is part of a fake review associated with a blackmailing buyer or vendor engaged in unfair competitive practices. If buyer ratings come into play due to popular demand, this is another means by which law enforcement could attack the reputation of cryptomarket users to lemonize the market (Yip et al., 2013).

Another finding with important implications for law enforcement interventions is the centrality of marketplace forums to conflict management on a cryptomarket. For example, targeting these forums by ostracizing trusted vendors or providing inaccurate advice on operational security has direct benefits, including a reduction in the trade of illicit goods and service and the apprehension of more users, respectively. Even more importantly though, these activities can bring the legitimacy of the forum into question, thereby crippling one of the most powerful and dynamic platforms for conflict management. Marketplace administrators may become less likely to consider the suggestions of other users; buyers may be less likely to heed warnings from other users that a vendor is a scammer.

These findings and conclusions should be interpreted in light of three major limitations affecting the validity of this study. First, only publicly available content was collected from TFM and WSM, precluding me from examining off-market forums and reaching out to users to conduct interviews with them. Forums such as Dredd are popular for users to complain about negative experiences on markets because of their perceived impartiality (i.e., cryptomarket staff cannot suppress dissent by removing comments and banning members). The fact that so much conflict management takes place behind closed doors through the support ticket system and staff-facilitated arbitration means that a large piece of the puzzle is missing which can only be obtained through personal interviews or other forms of interaction. Morselli et al. (2017) were able to justify their use of public data because the marketplace they studied, unlike TFM and WSM, used forums as the primary means of conflict resolution. Thus, discourse analysis, at least in isolation, may not be the best method to address the research question in this study. Triangulation with these other methods and data sources would substantially improve the validity of data and subsequent analysis.

Second, these two marketplaces lack generalizability to all kinds of markets. Although part of the appeal in selecting TFM and WSM was the diversity of offerings which are hoped to generate a range of conflict resolution / prevention content representative of multiple market types, each marketplace banned the sale of certain products. Most notably, child abuse content is banned on both cryptomarkets, but has been found by some researchers to account for the highest portion of dark web traffic compared to other materials (Chertoff, 2017). It is unknown whether these users differ significantly from those using marketplaces such as TFM or WSM, and whether this has an impact on how conflict management occurs.

Finally, the manual collection of data used in this study is inherently limited. While I endeavoured to be purposive and comprehensive, automated collection techniques are far more desirable since they can retrieve substantially more content in much less time (Aldridge & Decary-Hetu, 2015). For example, Moeller et al. (2017) initially collected 2.6 million forum posts and systematically reduce this to 404 161 posts based on a vocabulary of 4688 terms. While I would still have to look through each datum, the amount of time saved from not having to manually record each forum post would have enabled me to spend more time analyzing a wider range of content. Future research should use automated data collection techniques.

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. doi:https://doi.org/10.1016/j.drugpo.2016.10.010

Aldridge, J., & Decary-Hetu, D. (2015). Sifting through the net: Monitoring of online offenders by researchers. *European Review of Organised Crime*, *2*(2), 122-141. Retrieved from: https://www.researchgate.net/profile/Judith_Aldridge/publication/312446591_Sifting_through_the_net_Monitoring_of_online_offenders_by_researchers/links/5885c6a9a6fdcc6b79190281/Sifting-through-the-net-Monitoring-of-online-offenders-by-researchers.pdf

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, *2*(1), 26-38. doi:10.1080/23738871.2017.1298643

DeepDotWeb. (2019). Top markets! Retrieved from ttps://www.deepdotweb.com/marketplace-directory/categories/top-markets/

Dolliver, D. S., & Kennedy, J. L. (2016). Characteristics of drug vendors on the Tor network: A cryptomarket comparison. *Victims & Offenders, 11*(4), 600-620. doi:10.1080/15564886.2016.1173158

Hesse-Biber, S. N. (2017). *The practice of qualitative research: Engaging students in the research process* (3rd ed.). Thousand Oaks, CA: SAGE Publications.

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice, 14*(3), 351-367. doi:10.1177/1748895813505234

Martin, J., & Christin, N. (2016). Ethics in cryptomarket research. *International Journal of Drug Policy*, *35*, 84-91. doi:https://doi.org/10.1016/j.drugpo.2016.05.006

Moeller, K., Munksgaard, R., & Demant, J. (2017). Flow my FE the vendor said: Exploring violent and fraudulent resource exchanges on cryptomarkets for illicit drugs. *American Behavioral Scientist*, *61*(11), 1427-1450. doi:10.1177/0002764217734269

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict management in illicit drug cryptomarkets. *International Criminal Justice Review*, *27*(4), 237-254. doi:10.1177/1057567717709498

Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2016). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy, 35*, 58-68. Retrieved from http://dx.doi.org/10.1016/j.drugpo.2015.12.010

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. doi:http://dx.doi.org/ 10.1016/j.drugalcdep.2017.01.004

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, *23*(4), 516-539. doi:10.1080/10439463.2013.780227