American Behavioral Scientist
1–17

DOI: 10.1177/0002764217734265
journals.sagepub.com/home/abs


Are Repeat Buyers in Cryptomarkets Loyal Customers? Repeat Business Between Dyads of Cryptomarket Vendors and Users

David Décary-Hétu[1,2] and Olivier Quessy-Doré[1]

Abstract

Organizations involved in the sale of illicit products and services have been described as small, ephemeral, and local rather than global. Given their limited size, such organizations are often unable to attract large pools of customers, but it has been noted that organizations that manage to build a small but loyal customer base are likely to be more secure and to incur fewer risks of arrest and victimization. There has been little previous research into the loyalty of repeat buyers on Internet markets but a new technological innovation, cryptomarkets, makes it now more possible to track transactions between vendors and their customers. This article looks at the level of loyalty of cryptomarket repeat buyers by tracking their purchases over time. We find that, on average, customers make 60% of their purchases from the same vendor and that providing increased amounts of information to customers increases the loyalty of cryptomarket vendors' customer base.

Keywords

loyalty, cryptomarkets, competition

[1]School of Criminology, University of Montreal, Montreal, Quebec, Canada
[2]International Centre for Comparative Criminology (ICCC), University of Montreal, Montreal, Quebec, Canada

Corresponding Author:
David Décary-Hétu, School of Criminology, University of Montreal, 3150 Jean-Brillant, Montreal, Quebec, H3C1J7, Canada.
Email: david.decary-hetu@umontreal.ca

Online Illicit Markets and Cryptomarkets

The Internet has proven to be an efficient tool to facilitate economic transactions. While most individuals use it to purchase legal products such as books, clothes, and electronic devices, some also use it to facilitate the sale and purchase of illegal products such as credit cards (Motoyama, Mccoy, Levchenko, Savage, & Voelker, 2011; Décary-Hétu & Leppänen, 2016) and hacking tools and software (Holt, 2013). Until recently, many of these sales took place though discussion forums and chatrooms where vendors and buyers could exchange messages (Décary-Hétu, 2013). However, a criminal innovation, known as a *cryptomarket* (Martin, 2014a), now provides a new platform for such transactions that increases the security of users and provides a safer way to buy a new range of illicit products, such as illegal drugs. A cryptomarket is "a marketplace that hosts multiple sellers or 'vendors', provides participants with anonymity via its location on the hidden web and use of cryptocurrencies for payment, and aggregates and displays customer feedback ratings and comments" (Barratt & Aldridge, 2016, p. 1). Such markets resemble websites such as eBay in that their products are shown in a list of pictures with a single detailed web page created for each listing and each vendor. Just as on eBay, any individual or organization can create a vendor account and put up goods and services for sale (Christin, 2013). There appears to be only minimal vetting of vendors as anyone who is willing to pay an account creation fee or place money in escrow to refund customers' money in case of fraud can use an automated form to create a vendor account.

Cryptomarkets are reachable only through a "free circuit-based low-latency communication service" called Tor (Dingledine, Mathewson, & Syverson, 2004, p. 1), and are thus able to conceal their participants' identity and location, resulting in greater anonymity than the Internet usually provides (Martin, 2014a). The use of cryptocurrencies such as bitcoin helps evade banking oversight and makes it very difficult to track payments back to a specific individual (Christin, 2013). Cryptomarkets also allow vendors to reach a large number of potential buyers without attracting much attention from the police (Aldridge & Décary-Hétu, 2014; Barratt, Ferris, & Winstock, 2014; Martin, 2014b). Automated reputation systems are used to regulate interactions between vendors and buyers: buyers are strongly encouraged to leave feedback and rate their purchasing experience (Soska & Christin, 2015). The authors' personal experience with cryptomarkets is that while providing feedback after a transaction is not mandatory, it is often strongly encouraged by cryptomarket administrators.

There are now over a dozen large cryptomarkets in operation (Kruithof et al., 2016). While at first they were involved mainly in the sale of illicit drugs—and most sales still involve illicit or prescription drugs—they have now diversified their activities to include hacking services, stolen financial information, and fake or stolen identity papers (Décary-Hétu, Mousseau, & Rguioui, 2017). Like cellphones, cryptomarkets have significantly changed the way drug dealers interact with their customers. Research has shown that there are fewer threats and violent episodes linked to drug dealing online than to such deals made offline (Barratt, Ferris, & Winstock, 2016), possibly because the identity of participants is protected on cryptomarkets. Such research has

also suggested that producers can now reach consumers directly, allowing for fewer intermediaries, more affordable prices, and higher drug quality (Martin, 2014b). While these last conclusions need to be validated, there has been a sharp rise in the use and adoption rate of cryptomarkets (Kruithof et al., 2016; Soska & Christin, 2015), with annual revenues estimated to be in the hundreds of millions of dollars per year.

Loyalty

Cryptomarkets' main feature is the facilitation of secure transactions between vendors and buyers. While some vendor–buyer relationships may be ephemeral, it is possible that others evolve into strong, loyal, and durable relationships. In economic terms, loyalty is defined as a buyer's tendency to choose to repeatedly make purchases from the same vendor even when other vendors are available. At its simplest level, the concept includes two core elements: a repeated behaviour and a favourable attitude toward a vendor (Anderson & Srinivasan, 2003; Oliver, 1997). In terms of behaviour, loyalty is shown by multiple transactions with the same vendor at different points in time. The temporal aspect ensures that mere convenience is not enough to explain the repeated purchases (Oh & Parks, 1997) and that a buyer decides whether to repeat the experience of purchasing a product from a vendor. Loyalty also means that the purchaser will choose to buy from a particular vendor even if alternative ways of acquiring the desired product are available. It indicates a buyer's preference for a vendor, especially when other offers appear preferable (Anderson & Srinivasan, 2003; Oliver, 1997). Loyalty does not, however, always mean exclusivity: buyers who make most of their purchases from a single vendor should still be considered loyal (Neal, 1999).

The rise of online markets has made loyalty an important consideration for vendors. Online markets reduce the number of interactions between vendors and buyers, limiting opportunities for vendors to negotiate and to convince buyers to make another purchase (Castaneda, 2010). The open nature of online markets also makes it easier for buyers to compare products and to find new suppliers. Online vendors must therefore compete with suppliers that may be more convenient or more skilled at attracting buyers (Balabanis, Reynolds, & Simintiras, 2006). Online markets also create new issues for buyers as they can neither meet vendors directly nor see and touch the products they are interested in (Ba & Pavlou, 2002). In this context, expectations are more likely to be disappointed, misunderstandings more likely to happen, and trust more likely to be abused.

A range of factors affect the decision to remain loyal to a vendor, some of which come into play before the purchase is made (Valvi & Fragkos, 2012). External factors such as competition and reputation as well as internal factors such as a buyer's characteristics or familiarity with a product affect the possibility that a buyer will purchase from a different supplier in the future (Valvi & Fragkos, 2012). The purchase itself can also affect buyer loyalty—an uncomplicated and pleasant experience is much more likely to result in a buyer deciding to deal with a known vendor (Chiu, Chang, Cheng, & Fang, 2009). The outcome of a purchase also influences a buyer's loyalty. Buyer satisfaction (Anderson & Srinivasan, 2003; Castaneda, 2010; Oliver, 1997), trust (Ba

& Pavlou, 2002), the perceived value of a purchase (Valvi & Fragkos, 2012), and convenience motivation (Valvi & Fragkos, 2012) are determinant when it comes to loyalty. Satisfaction is related to the enjoyment that the product procures and is closely related to whether the purchase meets buyer expectations (Oliver, 1997). It is the concept most closely correlated to loyalty, making it an essential goal for a vendor. Trust is another major component of loyalty: Buyers must feel that the information traded or the product purchased will not have unforeseen negative consequences and that the product is as described. Perceived value refers to the feeling that payment and purchase are either of equal value or that the buyer came out on top in the transaction (Oliver & DeSarbo, 1988; Valvi & Fragkos, 2012). Finally, convenience motivation relies on the tendency of online buyers to see convenience and a low level of effort as extremely important, sometimes playing a bigger role in their decision to shop online than saving money (Anderson & Srinivasan, 2003; Valvi & Fragkos, 2012).

The Loyalty of Cryptomarkets Customers

Illicit drug market participants are known for their ability to adapt (Bouchard, 2007; Caulkins & Reuter, 1998; Hoffer, Bobashev, & Morris, 2009) and cryptomarkets are the latest innovation in their attempts to increase the security of their operations and the ease with which they can conduct transactions with buyers. Illicit organizations are wary of law enforcement agencies (Reuter, 1983) and have in general have limited the size and scope of their operations (Bouchard & Ouellet, 2011; Eck & Gersh, 2000), and have focused on controlling only a small share of each illicit market (Reuter, 1983), remaining small, ephemeral, and local as opposed to global in order to survive. Eck and Gersh (2000) describe one type of illicit market, the illicit drug business, as a cottage industry in which drugs are "supplied by a large number of free-lance traffickers, rather than by a few, large scale organizations" (p. 263). In many economic settings, a small customer base limits growth and profits (see, for example, Fuentelsaz, Garrido, & Maicas, 2012; Maicas & Sese, 2015; Shankar & Bayus, 2003), but criminal organizations often cannot afford to seek and maintain relationships with a large number of partners or clients. The lack of human resources forces organizations to prioritize certain ties over others, thereby limiting the number of customers. Having a limited number of relationships also allows for the creation of stronger ties, which may reduce the risk of denunciation, arrest, and violence. In this sense, building a small and loyal customer base helps organizations operate in a more secure and efficient way and moves them toward the secure end of the efficiency–security trade-off (Morselli, Giguère, & Petit, 2007). Such organizations do not aim at the highest monetary return but profit instead from having a smaller pool of clients (Bouchard, 2007; Bouchard & Ouellet, 2011). Such organizations are also more likely to adopt new communication technologies (Bouchard, 2007; Hough & Natarajan, 2000; Ritter, 2005).

Past research has shown that illicit markets are competitive settings (Desroches, 2007; Reuter, 2009; van Duyne, 1996) and that buyers are likely to be attracted to dealers who can provide a product at lower cost. Vendors actively seek to attract buyers away from each other, even using marketing techniques such as branding or price

decreases (Goldstein et al., 1984). Because of the illegal status of illicit markets, there has been little research on the loyalty level of illicit market participants or the characteristics that help vendors build a more loyal customer base. Aldridge and Askew (2016) addressed this topic indirectly in their article on the self-presentation of drug vendors on SR1 and found that vendors actively sought to secure long-term relationships with customers through shipping and refund policies. The present research, building on this past research, takes advantage of the move of illicit markets in drugs to cryptomarkets to use the automated feedback system that tracks transactions between cryptomarket vendors and buyers as a way to analyze the loyalty of illicit market participants. To do so, we first map the business ties between the vendors and repeat buyers. Buyer names are somewhat anonymized by cryptomarket administrators, so in the past it has been difficult to connect vendors and buyers. We make use of a new methodology that allows us to uncover the hidden ties between them. Our second aim is to determine the characteristics that affect the loyalty of repeat buyers through an analysis of the number of vendors they purchase from. Finally, we create a predictive model that indicates whether vendors are able to generate loyalty among repeat buyers. This model factors in the self-presentation and experience of vendors to explain why certain vendors receive more repeat business. We are able to provide a better understanding of the relationship between repeat buyers and vendors in the context of cryptomarkets, enabling us to understand how repeat buyers behave when they have access to a wide variety of illicit products for purchase. This research thus contributes to the literature on competition in illicit markets and on networking between illicit market vendors and repeat buyers.

Data and Methods

To monitor the activities of cryptomarket participants, we developed a custom software tool called DATACRYPTO (Décary-Hétu & Aldridge, 2015). DATACRYPTO first logs into a cryptomarket and downloads its home page. It then parses that home page for hyperlinks to other pages hosted on the same website and sequentially visits each page, looking for more pages to download. Once it is unable to find new pages, DATACRYPTO switches to scraping mode and seeks to extract relevant information from each of the web pages it has downloaded. Of particular interest are pages that contain listings, vendor profiles, and feedback from participants. With listings, DATACRYPTO gathers product titles, product categories,[1] descriptions, prices, countries from which products are shipped (both to and from), as well as vendor usernames. In the case of vendor profiles, DATACRYPTO collects vendor usernames, dates of profile creation, profile descriptions, PGP keys,[2] average ratings from past buyers and vendor levels.[3] Feedback from participants, while not mandatory, is strongly encouraged following each transaction as this allows vendors to build an online reputation. Each feedback includes a listing identifier, the vendor username, a somewhat anonymized buyer username, a rating that varies from negative (0 points), to neutral (3 points), to positive (5 points), and the date the feedback was posted.

Table 1. Frequency Distribution of Abbreviated Usernames.[a,b]

Least frequent			Most frequent		
Username	Frequency	Weight	Username	Frequency	Weight
_**|	1	1.00	s**a	72,246	0.00
-**]	1	1.00	a**a	65,199	0.10
-**C	1	1.00	m**a	62,184	0.14
-**D	1	1.00	s**n	57,271	0.21
-**E	1	1.00	k**a	54,699	0.24

[a]A total of 418 abbreviated usernames had a frequency of *1*. The first five in alphabetical order are presented in Table 1. [b]The formula to calculate the weights is $W = 1 - (I_f/X_f)$ where W is the weight, I_f is the frequency of I and X_f is the frequency of X, the abbreviated username that appears with the greatest frequency.

While DATACRYPTO can be used to collect data from multiple cryptomarkets, this article focuses on a single cryptomarket,[4] selected based on two considerations. First, it is one of the most active, with 15,873 listings from 1,135 vendors when the data were collected in September 2015, thus providing a fairly representative picture of the current state of illicit activities on cryptomarkets. Second, it provides the best information among all cryptomarkets regarding the relationships between vendors and buyers. While most cryptomarkets hide the identity of the participants who post feedback, the cryptomarket we selected provides the first and last character of the username of the participant separated by two asterisks, no matter the length of the username (ex: *s**a*), for each feedback. The first and last character can be lowercase letters, uppercase letters, numbers, or special characters. As there are 76 possible characters, a total of 5,776 different possible abbreviated usernames are available. Our population included 1,826 different abbreviations, so it is possible that more than one buyer was represented by the same abbreviated username. To account for this possibility, a weight was associated to each repeat buyer, based on the likelihood that the username was unique. Repeat buyers with a higher weight were much more likely to be unique and weighed more in our analyses. To calculate the weights, we ran a frequency distribution on a list of 10 million usernames, published by Mark Burnett,[5] that had been created using multiple website leaks in which usernames were published. Table 1 presents the most and the least frequent abbreviated usernames.

Abbreviated usernames found only once in the 10 million list were given a weight of 1. At the opposite end, abbreviated usernames that were found tens of thousands of times were thought to be more common and therefore given a much smaller weight.

The weighted abbreviated usernames were used in the first part of our analyses to measure the loyalty from the repeat buyers' side. As defined in the literature, loyalty is the act of purchasing from the same person on multiple occasions. Loyalty was therefore measured in two ways: the average number of vendors used by a repeat buyer and the average largest share of transactions made by repeat buyers that went to a single vendor. As repeat buyers were likely to purchase more than one type of product, this

methodology was applied to all purchases made by repeat buyers as well as to purchases made in a single product category. In the latter case, a repeat buyer was believed to be loyal if he or she purchased all of his or her cannabis from a single vendor and all of their cocaine from another single vendor. In all cases, only repeat buyers who made more than one purchase were selected. In all, 91% of those identified by anonymized buyer names made more than one purchase.

In the second part of our analysis, the point of view of vendors was taken and a linear regression was used to predict the loyalty of vendors' customers. The dependent variable was the averaged loyalty score for each vendors' repeat buyers, calculated for each category in which the vendor sells. Only vendors with buyers who made at least two purchases were included in the sample. The independent variables included vendor characteristics, strategies, and network. Vendor characteristics include the vendors' *experience* as indicated by the number of days between their registration date with the site and the date of data collection. They also include their *rating* as well as their *vendor level*. Vendors' strategies include the *length of their profile description* and the *average length of their listing descriptions*. Measured in number of characters, the length of a description is likely to be a good proxy for the amount of information that a vendor shares with potential buyers. We expected that vendors who operate in an open fashion, sharing more information, were more likely to have more loyal customers. Vendors' strategies also include the *number of listings* and their *degree of diversification* based on the number of categories in which they offer products. Combined, these two variables enable us to determine if vendors who sell a small number of products (low diversity) but have many listings have customers who are more loyal. Multiple listings probably mean that a vendor offers not only different varieties of the product but the same product in different amounts, since each listing has only one quantity and one price associated with it. We expected that vendors who share an *email address* are more open and would be more likely to have loyal customers. Finally, vendors' networking includes the size of their transaction network based on the *number of buyers*. Table 2 presents the descriptive statistics of the variables included in the model.

Table 2 shows that the loyalty of repeat buyers varies greatly between vendors. Some vendors have only loyal repeat buyers (maximum = 100%) while others have a hard time keeping their repeat buyers (minimum = 3%). On average, vendors post 12 listings and sell 3 types of products. Around 30% of vendors include a public email address as part of the descriptions on their listing pages or in their vendor profile. The length of descriptions on listing pages varies greatly, with some going up to 32,000 characters. Almost all vendors have an excellent rating, with the average 4 out of 5 stars and a small standard deviation of 0.4. Most vendors have made only a few past sales, as indicated by their low vendor level ($M = 1$). Vendors have on average 113 days (4 months) of experience and during that time have received orders from 26 buyer usernames.

Results

Cryptomarkets are known to host many transactions and Figure 1, which shows the distribution of transactions on a single cryptomarket, gives an idea of just how

Table 2. Descriptive Statistics of the Predictive Model Variables.

	N	Minimum	Maximum	Mean	*SD*
Loyalty (percentage)	503	3%	100%	36%	19%
Number of listings	503	1	89	12	13
Degree of diversification	503	1	9	3	2
Public email address	503	0.0	1.0	0.3	0.5
Average product description length	503	23	19,817	1,007	1,478
Profile length	503	0	32,722	2,976	3,646
Average rating	503	0.0	5.0	4.0	0.4
Vendor level	503	1	7	1	1
Experience (days)	503	1	274	113	62
Number of clients	503	1	292	26	41

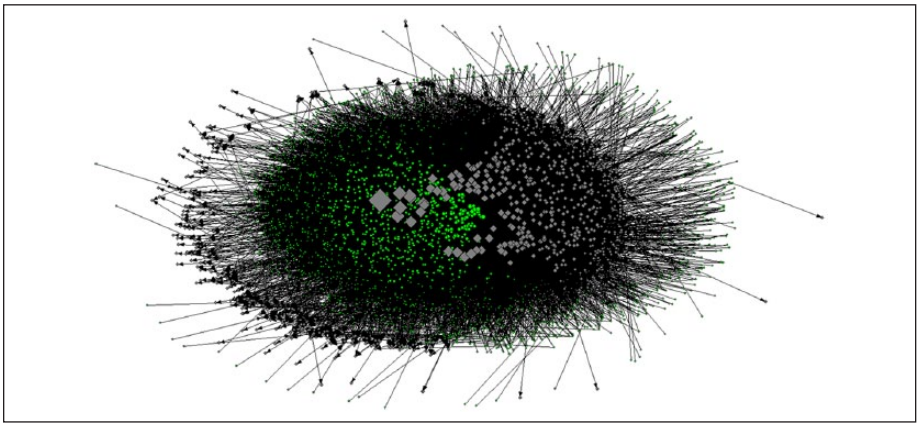

Figure 1. Distribution of transactions.

decentralized these markets are. Each node represents a cryptomarket participant; vendors are indicated in gray and repeat buyers in green. The size of the nodes reflects the number of sales made by a vendor. Each line represents a transaction between a vendor and a repeat buyer.

The high number of actors and transactions makes it difficult to identify patterns in the transactions but some vendors are clearly at the periphery of the network with very few incoming ties. These are the actors at the fringe of the sociogram. Vendors with the most sales (largest nodes) are clustered at the heart of the network. This visualization of cryptomarket transactions demonstrates that sales are distributed among vendors and that some vendors are clearly able to generate more sales than others as indicated by the varying size of the nodes. This does not mean that more active vendors have a loyal customer base but only that some vendors make more sales than others. Table 2 presents the first results of analyzing loyalty from the repeat buyers' point of view.

Table 3. Loyalty of Cryptomarket Repeat Buyers.

	Minimum	Maximum	*M*	*SD*
Number of vendors (per repeat buyer)	1	126	15	18
Share of purchases going to most frequently used vendor (per repeat buyer)	3%	100%	31%	21%
Number of specific categories purchased in (per repeat buyer)	1	27	7	5
Number of vendors purchased from per specific category (per repeat buyer)	1	9	3	1
Share of purchases going to most frequently used vendor per specific category (per repeat buyer)	17%	100%	58%	20%

Table 3 shows that on average repeat buyers made purchases from 15 vendors. That number varied considerably, with some repeat buyers dealing with up to 126 vendors (*SD* = 18). This suggests that cryptomarket relationships are not dyadic in nature, at least for repeat buyers who have made more than one purchase. The largest percentage of transactions going to a single vendor varied from 3% to 100%. On average, repeat buyers concentrated almost a third of their purchases with a single vendor (*M* = 31%), although again this average may not be representative, given the range of concentration (*SD* = 21%). Looking at transactions on a specific category basis, repeat buyers appear to make purchases across multiple categories (*M* = 7). This is not surprising, given the wide array of products available on cryptomarkets. It is also possible that some of the repeat buyers are sellers themselves and are looking to acquire their stock on line (Aldridge & Décary-Hétu, 2016), especially when we consider the number of different categories bought by a single vendor (maximum = 27). The average number of categories of products bought by a repeat buyer appears to be more representative in this case (*SD* = 5). When we look at the activities of repeat buyers in each specific category, we find that repeat buyers use a much more limited set of vendors, making purchases on average from three vendors in each specific category (minimum = 1; maximum = 9). Purchases in a specific category were almost twice as concentrated as general purchases (58% of purchases going to a single vendor vs. 31%). The share of purchases from a single vendor for a specific category varies between 17% and 100%, suggesting that some repeat buyers make all of their purchases from the same vendor.

The regression model presented in Table 4 describes the factors that affect the loyalty level of a vendors' repeat buyer's base. Our results suggest that the amount of information provided by a vendor in profile and listing description is significantly and positively correlated with the average level of loyalty of a vendor's customer base. Vendors who share more information attract a more loyal customer base. Offering a means to contact the vendor outside of the cryptomarket, such as by posting a public email address, is not significant. This suggests that repeat buyers do not feel the need to use out-of-band communication methods but find the communication mechanisms

Table 4. Predicting the Loyalty of Repeat Buyers.

	B	*SE*	β	*t*	Significance
(Constant)	23.382	10.940		2.137	.033
Number of listings	0.125	0.081	0.086	1.548	.122
Degree of diversification	0.282	0.566	0.026	0.499	.618
Public email address	0.020	1.814	0.001	0.011	.991
Average description length (logged)	1.518	0.756	0.094	2.009	.045
Profile length (logged)	−1.301	0.608	−0.102	−2.141	.033
Average rating	1.588	1.883	0.038	0.844	.399
Vendor level	0.045	1.689	0.002	0.027	.979
Experience (days)	0.014	0.014	0.048	1.033	.302
Number of clients	0.038	0.040	0.083	0.954	.341

built into the cryptomarkets sufficient. None of the other variables in the model was statistically significant. Some of these results were surprising, especially in the case of the vendors with a higher vendor level, vendor rating, and experience. It appears that more established vendors do not foster more loyalty than others among cryptomarket repeat buyers. Exposure and visibility on cryptomarkets through a higher number of listings is also not correlated to a more loyal customer base. Finally, the vendors with the largest customer base are also not more likely to have a more loyal customer base.

Discussion and Conclusion

This research takes advantage of the rise of cryptomarkets and the wealth of information they store on their sites to characterize the level of loyalty in an illicit online cryptomarket. Our results suggest that few repeat buyers are totally loyal to a specific vendor. In some cases, repeat buyers may want to remain loyal to a vendor but are forced to purchase from other vendors when their main vendor is unable to supply them with the products they want. In other cases, there may be several reasons for repeat buyers to decide to buy from a different vendor even when their main vendor is available. First, repeat buyers may want to build multiple relationships to limit their dependence on their main vendor. Police operations, scams, holidays, and sourcing issues can all prevent a vendor from being able to deliver goods and services for a certain period. Moreover, Reuter (1983) has shown that criminal organizations are usually ephemeral, a statement confirmed by our descriptive analyses of the experience of vendors and past research by Christin (2013). Vendors can disappear without notice. In this context, it makes sense for repeat buyers to use more than one vendor. Second, repeat buyers may be tempted to buy from vendors who are providing products that are either cheaper or whose quality is advertised as being superior. Hundreds of vendors are competing on cryptomarkets at any given point in time (Soska & Christin, 2015) and it is very possible that their marketing campaigns will lead repeat buyers to make a purchase from a new vendor. Third, establishing relationships with

different vendors may help repeat buyers establish their trustworthiness on cryptomarkets. Vendors usually require that customers making their first purchase provide payment before the product is shipped as scammers have been known to register new accounts, order products online, receive their products, and then claim that they never received them and ask for a refund. As there are no fees for registering a buyer's account, scammers could in theory repeat this strategy again and again, using new shipping addresses and new vendors. Even though the high rating of most vendors suggests that cryptomarkets are populated with relatively reliable vendors, repeat buyers still take some risk when they release payment to a vendor before their products have been shipped. By purchasing from multiple vendors, repeat buyers can use the unofficial vouching system in which a repeat buyer tells a new vendor that they have purchased from another vendor in the past and leaves it to the new vendor to either contact that vendor or simply accept the buyer's statement and eliminate the need for payment before shipment (finalize early in cryptomarket terms).

While repeat buyers also make purchases from other vendors, on average they make about 60% of their purchases in each product category from the same vendor. To be considered loyal, repeat buyers do not have to make all of their purchases from the same vendor (Neal, 1999) but only make a large portion of their purchases from the same source when alternatives are available. Past research (Ba & Pavlou, 2002; Balabanis et al., 2006; Castaneda, 2010) suggests that some features of online relationships reduce the loyalty of customers. While it is difficult to compare the loyalty level of offline and online buyers of illicit products and services, being loyal to a single vendor makes sense both offline and online. Having a main supplier may protect repeat buyers from the risks associated with buying from an unknown supplier. Costs of switching buyers include the possibility of denunciation by the previous vendor, sending payment without receiving the product, and receiving a product that is not what is expected and may even be dangerous (Skott & Jepsen, 2002). Undercover agents are unlikely to maintain a fake illicit business for an extended period and buyers who have long-lasting relationships are better able to protect themselves from arrest. Being a repeat buyer also reduces the asymmetry of information (Akerlof, 1970) and allows the vendor to know what to expect from a buyer.

Not all vendors manage to build a loyal customer base. Those that do appear to do so by providing more information about their products and themselves in their descriptions. Surprisingly, the online reputation of vendors does not appear to play a significant role in the ability of vendors to create a loyal customer base, in contrast to legitimate markets where research has found that reputation and past satisfaction increase customer loyalty (Anderson & Srinivasan, 2003; Castaneda, 2010; Oliver, 1997; Valvi & Fragkos, 2012). This difference may be a result of the low variance between *vendor rating* and *vendor level* variables. In line with previous research (Christin, 2013), we found that about 95% of feedback posted on the cryptomarket was positive, with only about 1.5% negative. Ratings do not vary much across vendors, limiting the possibility of linking ratings to a loyal customer base. About 70% of vendors were also relatively new and had a vendor level of 1, the level all vendors get when they register an account. Further qualitative research should investigate the role

that vendor rating and vendor level play in the decision of repeat buyers to purchase from one vendor rather than another. A qualitative approach is more suitable to identifying the relevance of these variables as it can look at how repeat buyers see vendors. Reputation can also be expressed in terms of experience as vendors who have been active for a long time may be seen as more reliable. However, this was not the case in our regression model as experience did not significantly affect the loyalty of a vendor's customer base. It is possible that the competition on cryptomarkets is so fierce that repeat buyers will tend to seek new vendors over time and more experienced vendors will therefore have a pool of repeat buyers who have made purchases from other vendors. As it does not cost anything to maintain a vendor profile, it is also possible that our results were tainted by including several vendors who had stopped responding to buyers, forcing them to seek new vendors.

A large pool of repeat buyers and a diversification of products offered for sale does not translate to a more loyal repeat buyer base. It is possible that having a large number of clients limits the time that vendors can spend making sure their clients are satisfied with their service. For instance, it may take such vendors more time to answer messages and to ship packages. Given the small size of criminal organizations (Bouchard & Ouellet, 2011), having a large pool of clients may actually be a problem for those vendors who lack the human resources to provide service. Chiu et al. (2009) found that an uncomplicated and pleasant experience is much more likely to result in a client inclined to deal with a known vendor: A large pool of clients may prevent vendors from providing a pleasant experience to their customers. We expected that vendors who offered many types of products would be able to take care of all their clients' needs so that they would not have to seek other vendors, thus creating a more loyal customer base, but that does not appear to be the case. It is possible that vendors who specialize can offer better prices and repeat buyers may purchase from specialists to get the most value.

This article is a rare empirical foray into the loyalty of cryptomarket repeat buyers. Given the illicit nature of their activities, offenders are not always willing to discuss openly how they operate. Recall of past activities may also be problematic after a certain period, making the availability of cryptomarkets data an interesting development for social science research. The main limit of such research is that public feedback does not contain the username of specific buyers but only the first and last character of a username, making it possible that many buyers are identified by the same first and last characters. If this is the case, the number of buyers associated with each vendor is higher than shown, making the loyalty of repeat buyers higher than reported. Further analyses should take a more qualitative approach and survey online buyers about their loyalty. Individual surveys would make it possible to obtain much more precise data on the buying habits of cryptomarket participants and provide more understanding of this important concept. The present article contributes to the cryptomarket literature by designing a new and innovative methodology that gives a different weight to buyers depending on the likelihood of overlap between two buyer names. This methodology opens the door to new research, especially in social network analysis. Past research was hampered by difficulty in identifying buyers but this method makes it possible to model how buyers network with vendors.

Given the level of loyalty found in our analyses, it is not surprising that most feedback left with vendors on cryptomarkets is positive. Repeat buyers appear to have a main supplier from whom they make about 60% of their purchases in each specific product category and the presence of these strong ties may have a positive effect on the experience of both repeat buyers and vendors, contributing to the growth of cryptomarkets. Cryptomarkets have grown consistently over the past years (Kruithof et al., 2016) and the few police operations that have targeted them did not have a lasting effect on their activities (Décary-Hétu & Giommoni, 2016). Strong ties between repeat buyers and vendors may contribute to the continued operations of cryptomarkets by raising the trust that cryptomarket actors have in each other. Regulators and offenders may therefore have to deal with the online sale of illicit products and services for the foreseeable future and this new reality should be taken into account when regulations and prevention programs are designed. Cryptomarkets may make it possible to purchase drugs with less risk (Barratt et al., 2016) and loyalty may play a role in increasing the harm reduction benefits cryptomarkets provide to online illicit markets.

Appendix

List of Categories

Drugs

- Benzodiazopines
- Cannabis and hashish
- Dissociatives
- Drugs (not specified)
- Ecstasy
- Opioids
- Paraphernalia
- Prescription drugs
- Psychedelics
- Steroids
- Stimulants
- Tobacco
- Weight loss

Financial fraud

- Accounts and bank drops
- Carding
- CVV and cards
- Dumps
- Gold
- Money

Fraud

- Fake IDs
- Fraud
- Fraud software
- Personal information and scans

Computer security

- Appliances (virtual machines)
- Botnets and malware
- Exploit kits
- Exploits (software)
- Hacking (software)
- Hosting
- Security and anonymity (software)
- Security software
- Social engineering
- SOCKS Proxies
- Virtual private networks

Weapons

- Ammunition
- Explosives
- Long-range guns
- Pistols
- Weapons

Other

- Clothing
- Digital products
- E-books
- Electronics
- Jewelry
- Legitimate software
- Unknown
- Video game keys

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 the following financial support for the research, authorship, and/or publication of this article: Funding for this research was provided by the FRQSC (2016-NP-189347) and the SSHRC (#430-2015-01089).

Notes

1. Categories are mutually exclusive and are divided into specific types. The appendix presents the categories as listed on the cryptomarkets. This article uses the vendors' own classification of their listings.
2. PGP stands for Pretty Good Privacy. A PGP key is an encryption tool that allows one to encrypt a message that can only be decrypted by its intended recipient.
3. Vendors move up levels as they engage in transactions. Vendors at Level 2, for example, have made at least 100 sales worth over US$1,500; vendors at Level 5 have made over 500 sales worth US$25,000. All vendors at Level 2 and higher must have at least 90% positive feedback.
4. To protect the identity of the cryptomarket participants, the cryptomarket analyzed is not named in this article.
5. See Goodin (2015) for more details on the username list.

References

Akerlof, G. A. (1970). The market for lemons: Qualitative uncertainty and the market mechanism. *Quarterly Journal of Economics*, *84*, 488-500.

Aldridge, J., & Askew, R. (2016, May). *When drug dealers can advertise: how drug cryptomarkets enable drug dealers to advertise*. Paper presented at the Annual Conference of the Society for the Study of Drug Policy. Sydney, New South Wales, Australia.

Aldridge, J., & Décary-Hétu, D. (2014). *Not an 'Ebay for drugs': The cryptomarket 'silk road' as a paradigm shifting criminal innovation*. Retrieved from http://ssrn.com/abstract=2436643.

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

Anderson, R. E., & Srinivasan, S. S. (2003). E-satisfaction and e-loyalty: a contingency framework. *Psychology & Marketing*, *20*, 123-138.

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly*, *26*, 243-268.

Balabanis, G., Reynolds, N., & Simintiras, A. (2006). "Bases of e-store loyalty: Perceived switching barriers and satisfaction. *Journal of Business Research*, *59*, 214-244.

Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy*, *35*, 1-6.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction*, *109*, 774-783.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy*, *35*, 24-31.

Bouchard, M. (2007). On the resilience of illegal drug markets. *Global Crime*, *8*, 325-344.

Bouchard, M., & Ouellet, F. (2011). Is small beautiful? The link between risks and size in illegal drug markets. *Global Crime*, *12*, 70-86.

Castaneda, J. A. (2010). Relationship between customer satisfaction and loyalty on the internet. *Journal of Business & Psychology*, *26*, 371-383.

Caulkins, J. P., & Reuter, P. (1998). What price data tell us about drug markets. *Journal of Drug Issues*, *28*, 593-612.

Chiu, C. M., Chang, C. C., Cheng, H. L., & Fang, Y. H. (2009). Determinants of customer repurchase intention in online shopping. *Online Information Review*, *33*, 761-784.

Christin, N. (2013, May). *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*. Paper presented at the 22nd International Conference on World Wide Web, Rio de Janeiro, Brazil.

Décary-Hétu, D. (2013). *Le capital virtuel* [The virtual capital] (Unpublished doctoral dissertation). School of Criminology, Université de Montréal, Montreal, Quebec, Canada.

Décary-Hétu, D., & Aldridge, J. (2015). DATACRYPTO: The dark net crawler and scraper [Computer software]. Authors.

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*, 55-75.

Décary-Hétu, D., & Leppänen, A. (2016). Criminals and signals: An assessment of criminal performance in the carding underworld. *Security Journal*, *29*, 442-460.

Décary-Hétu, D., Mousseau, V., & Rguioui, I. (2017). *Le trafic illicite de tabac sur les cryptomarchés* [Illicit tobacco trafficking on cryptomarkets]. Retrieved from http://daviddhetu.openum.ca/files/sites/39/2017/07/Decary-Hetu-et-al.-2017-Rapport-final-2.pdf.

Desroches, F. (2007). Research on upper level drug trafficking: A review. *Journal of Drug Issues*, *37*, 827-844.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router*. Retrieved from https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf.

Eck, J. E., & Gersh, J. S. (2000). Drug trafficking as a cottage industry. *Crime Prevention Studies*, *11*, 241-272.

Fuentelsaz, L., Garrido, E., & Maicas, P. (2012). A strategic approach to network value in network industries. *Journal of Management*, *41*, 864-892.

Goldstein, P. J., Lipton, D. S., Preble, E., Sobel, I., Miller, T., Abbott, W., . . . Soto, F. (1984). The marketing of street heroin in New York City. *Journal of Drug Issues*, *14*, 553-566.

Goodin, D. (2015). *Fearing an FBI raid, researcher publishes 10 million passwords/usernames*. Retrieved from http://Arstechnica.Com/Security/2015/02/Fearing-An-Fbi-Raid-Researcher-Publishes-10-Million-Passwordsusernames.

Hoffer, L. D., Bobashev, G., & Morris, R. J. (2009). Researching a local heroin market as a complex adaptive system. *American Journal of Community Psychology*, *44*, 273-286.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, *31*, 165-177.

Hough, M., & Natarajan, M. (2000). Introduction: Illegal drug markets, research and policy. *Crime Prevention Studies*, *11*, 1-17.

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade*. Retrieved from http://www.rand.org/pubs/research_reports/RR1607.html

Maicas, J. P., & Sese, F. J. (2015). Customer-base management in network industries: The moderating role of network size and market growth. *European Management Review*, *12*, 209-220.

Martin, J. (2014a). *Drugs on the dark net*. New York, NY: Palgrave Macmillan.

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

Morselli, C., Giguère, C., & Petit, K. (2007). The efficiency/security trade-off in criminal networks. *Social Networks*, *29*, 143-153.

Motoyama, M., Mccoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011, November). *An analysis of underground forums*. *Paper presented at the Internet Measurement Conference*, *Berlin, Germany*.

Neal, W. D. (1999). Satisfaction is nice, but value drives loyalty. *Marketing Research*, *11*, 20-23.

Oh, H., & Parks, S. C. (1997). Customer satisfaction and service quality: A critical review of the literature and research implications for the hospitality industry. *Hospitality Research Journal*, *20*(3), 35-64.

Oliver, R. L. (1997). *Satisfaction: A behavioural perspective on the consumer*. New York, NY: McGraw-Hill.

Oliver, R. L., & DeSarbo, W. S. (1988). Response determinants in satisfaction judgments. *Journal of Consumer Research*, *14*, 495-507.

Reuter, P. (1983). *Disorganized crime: The economics of the visible hand*. Cambridge: MIT Press.

Reuter, P. (2009). Systemic violence in drug markets. *Crime, Law and Social Change*, *52*, 275-284.

Ritter, A. (2005). *Monograph No. 08: A review of approaches to studying illicit drug markets*. DPMP Monograph Series: Turning Point Alcohol and Drug Centre. Retrieved from https://dpmp.unsw.edu.au/sites/default/files/dpmp/resources/DPMP%20MONO%208.pdf

Shankar, V., & Bayus, B. L. (2003). Network effects and competition: An empirical analysis of the home video game industry. *Strategic Management Journal*, *24*, 375-384.

Skott, P., & Jepsen, G. T. (2002). Paradoxical effects of drug policy in a model with imperfect competition and switching costs. *Journal of Economic Behavior & Organization*, *48*, 335-354.

Soska, K., & Christin, N. (2015, August). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. *Paper presented at the 24th USENIX Security Symposium*, *Washington, DC*.

Valvi, A. C., & Fragkos, K. C. (2012). Critical review or the e-loyalty literature: A purchase-centred framework. *Electronic Commerce Research*, *12*, 331-378.

van Duyne, P. C. (1996). The phantom and threat of organized crime. *Crime, Law, and Social Change*, *24*, 341-377.

Author Biographies

David Décary-Hétu is an Assistant Professor at the School of Criminology of the Université de Montréal. He has worked as a Senior Scientist at the School of Criminal Sciences of the Université de Lausanne and studies online illicit markets.

Olivier Quessy-Doré is a Masters student at the School of Criminology of the Université de Montréal.