Forensic Science International: Digital Investigation 36 (2021) 301093

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

Dark web in the dark: Investigating when transactions take place on cryptomarkets

Yoichi Tsuchiya [a, *], Naoki Hiramoto [b]

[a] Tohoku University, 41 Kawauchi, Aoba, Sendai, 980-8576, Japan
[b] Tokyo University of Science, 1-3 Kagurazaka, Shinjuku, Tokyo, 162-8601, Japan

A R T I C L E   I N F O

Article history:
Received 14 October 2020
Accepted 26 November 2020
Available online xxx

Keywords:
Cybercriminal
Drug economy
Crypto currency
Information security

A B S T R A C T

Online illicit marketplaces known as cryptomarkets have gained considerable attention from the media, government authorities, law enforcement agencies, and researchers. An increasing number of studies have investigated various aspects of these cryptomarkets' characteristics, such as product categories, sale volumes, and the number of listings and vendors. However, there is a gap in the literature regarding whether illegal transactions (of illicit drugs) take place during the day or week. This study fills this gap by tracing Bitcoin addresses associated with the six previously leading and most active cryptomarkets—Silk Road, Silk Road 2.0, Agora, Evolution, Nucleus, and Abraxas—to identify the specific timings of these transactions. This study reveals clear patterns of activity on the marketplaces. First, transactions more often take place at night in European countries (Germany, Netherlands, the UK), the US, and Canada, where the cryptomarket drug trade is most active. Second, there are more transactions on Mondays, Tuesdays, and Wednesdays, and fewer on Saturdays and Sundays. This indicates that the retail drug trade accounts for a large part of the cryptomarkets. Further, this study examines the impact of a cryptomarket policing effort known as Operation Onymous, and indicates that this policing effort only displaced users among these marketplaces and did not deter their activity, even in the short-term. It also suggests that Operation Onymous did not alter users' transaction patterns.

1. Introduction

Online illicit marketplaces known as cryptomarkets have gained considerable attention from the media, government authorities, law enforcement agencies, and researchers since Silk Road, the first successful dark web marketplace, was launched in February 2011. These new online marketplaces focus on anonymity and security to limit the risk of identification, though they share many aspects of legitimate online marketplaces, such as eBay (Christin, 2013). Two online anonymizing technologies led to the creation of cryptomarkets. The first is cryptocurrency (Bitcoin). Bitcoin is a fully decentralized digital currency based on blockchain (Nakamoto, 2008). Although all transaction records are public, Bitcoin payments are anonymous unless the Bitcoin addresses and transactions can be matched to actual identities. The second technology is the Tor network, in which users' messages are routed through a series of relays that serve as a buffer between the users and the websites that they visit (Dingledine et al., 2004). This makes it difficult to determine the location of the visitor of a website. Administrators of dark web sites can conceal the location of their website servers and thus avoid law enforcement agencies. After Silk Road was shut down and its operators were arrested in October 2013, numerous cryptomarkets have been launched and increased attention has been paid by the relevant authorities.

Numerous studies have collected data and measured activity on cryptomarkets to reveal their various characteristics. The most popular products for sale on cryptomarkets are illicit drugs (e.g., Soska and Christin, 2015; Tzanetakis, 2018). The vendors and listings on cryptomarkets have increased, and trade and purchase volumes have steadily increased accordingly (e.g., Soska and Christin, 2015; Broséus et al., 2017; Rhumorbarbe et al., 2016). Police intervention has had a limited impact on cryptomarket activity (e.g., Aldridge and Décary-Hétu, 2016; Van Buskirk et al., 2017; Décary-Hétu and Giommoni, 2017), which restricts the structure of the geographical trade networks of buyers and sellers (e.g., Norbutas, 2018; Van Buskirk et al., 2016a,b). Previous studies have

* Corresponding author.
E-mail addresses: yoichi.tsuchiya.a5@tohoku.ac.jp (Y. Tsuchiya), naoki.hiramoto.tus@gmail.com (N. Hiramoto).

https://doi.org/10.1016/j.fsidi.2020.301093
2666-2817/

Table 1
Summary of active periods and reason for closure.

Marketplace	Active period		Closure
Silk Road	January 31, 2011 to October 2, 2013	(976)	Shut down
Silk Road 2.0	November 6, 2013 to November 5, 2014	(365)	Shut down
Agora	December 3, 2013 to September 6, 2015	(643)	Voluntary exit
Evolution	January 14, 2014 to March 14, 2015	(425)	Scam
Nucleus	October 24, 2014 to April 13, 2016	(538)	Scam
Abraxas	December 13, 2014 to November 5, 2015	(328)	Scam

Notes: Active periods are from EUROPOL (2017a, 2017b). The numbers in parenthesis are days that marketplaces are open. Closure indicates reason for closure.

mainly revealed the cryptomarkets' ecosystem from the vendor/supply perspective. Some studies have investigated the characteristics and motivations of purchasers on cryptomarkets (e.g., Van Hout and Bingham, 2013; Van Buskirk et al., 2016a,b), yet few have attempted to uncover the characteristics of the cryptomarkets from the buyer/demand perspective.

Therefore, this study investigates the times that users access cryptomarkets and make transactions, answering the question of what time users buy illicit drugs and products. When do users make transactions in a given week—on their days off or on work days? Answers to these questions can reveal the characteristics of cryptomarkets, thus filling a gap in the literature, and provide implications for policy efforts.

This study thoroughly investigates cryptomarkets via Bitcoin transactions by focusing on Silk Road, Silk Road 2.0, Agora, Evolution, Nucleus, and Abraxas, which were the six largest and most active marketplaces in operation between 2011 and 2015. Identifying Bitcoin transactions on cryptomarkets provides the exact time at which a transaction took place because all records are publicly available. This approach overcomes the following drawbacks of web crawling, which has been widely used when examining cryptomarkets. First, the scraping method may not extract all the information because scraping is not always available. Second, because scraping identifies transactions based on buyers' feedback, it cannot capture exactly when that transaction happened. Third, the actual prices and quantities can be different from those listed. Finally, the feedback may not be timely, and scraping cannot cover the entire lifetime of a certain dark web market. Therefore, this established method's measurement errors are avoided through the use of Bitcoin transactions because the transaction records provide accurate information on the sales volume and date of each transaction.

Although the Federal Bureau of Investigation (FBI) has shut down various cryptomarkets, the impact of police intervention is limited due to the rapid recovery of illicit transactions on the dark web. Nevertheless, international policing efforts toward closing cryptomarkets involving pseudo-anonymous transactions are increasingly important measures against cybercrime. Previous studies have shown that these policing efforts have had a limited impact on vendors. While there were reductions in the number of product listings and vendors on cryptomarkets soon after some were closed down, within one month, many vendors had quickly migrated to other cryptomarkets and the number of listings and vendors exceeded that of before the policing operations (Décary-Hétu and Giommoni, 2017). However, little is known about how buyers respond to such operations. Therefore, this study also attempts to address how cryptomarket buyers react to an internationally coordinated policing effort.

By using simple heuristics to measure the transactions on the six marketplaces, this study reveals clear patterns of activity on these markets. First, there are more transactions on Mondays, Tuesdays, and Wednesdays and less transactions on Saturdays and Sundays. Second, transactions more often take place at night in European countries, the US, Canada, and Australia, where the cryptomarket drug trade is most active. This indicates that the drug trade for retail purposes accounts for a large part of the cryptomarkets. Further, this study examines the impact of a cryptomarket policing effort known as Operation Onymous, and indicates that this policing effort only displaced users among these marketplaces and did not deter their activity, even in the short-term. It also suggests that Operation Onymous did not alter users' transaction patterns.

The remainder of this paper is organized as follows. Section 2 provides an overview of related studies and background information on cryptomarkets. Section 3 describes the measurement method for identifying transactions on cryptomarkets. Section 4 presents the results, while Section 5 discusses the implications and limitations of the study. The conclusion is presented in Section 6.

2. Related work

Before providing a review of the related work, the background of the six cryptomarkets is briefly provided. Table 1 shows the active periods and reasons for closure of the six cryptomarkets that are investigated herein. The first successful cryptomarket, Silk Road, was launched in February 2011 and shut down in October 2013 after the FBI arrested its operators. After about a month, Silk Road 2.0 was launched, and again shut down by an international law enforcement operation known as Operation Onymous[1] in November 2014, which was undertaken by the FBI and the European Police Office (EUROPOL, 2017a). Among the many marketplaces, Agora, which operated between December 2013 and September 2015, and Evolution, which operated between January 2014 and March 2015, overtook Silk Road 2.0. Evolution evolved rapidly and became the largest dark web marketplace after Operation Onymous. Agora took the leading position after Evolution's exit scam (EUROPOL, 2017a), and was then closed voluntarily; Agora and Evolution were not shut down by Operation Onymous. Nucleus operated between October 2014 and April 2016, while Abraxas operated between December 2014 to November 2015. The two marketplaces[2] grew steadily, and were both involved in an exit scam.

Studies have provided evidence of these marketplaces' characteristics, including sales volume estimates and numbers of listings, vendors, and product categories, via scraping methods. These studies have revealed several aspects of cryptomarkets from vendors' perspectives because scraping methods collect information on feedback received by the vendors.

Soska and Christin (2015) scraped 35 marketplaces, including those investigated in this study (except Abraxas), and collected 78,509 item listings between 2013 and 2015. The overall annual

[1] See EUROPOL (2014) for details.

[2] Around the launch of these two marketplaces, AlphaBay was launched and became the most active marketplace. AlphaBay was not investigated due to limitations of data availability.

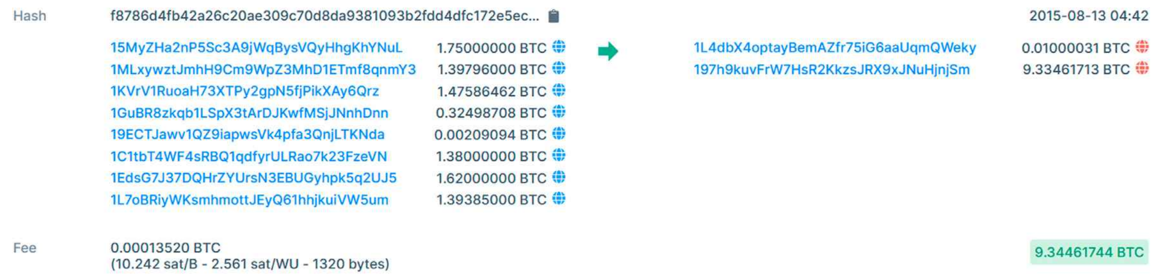


Fig. 1. Bitcoin transactions.

revenue was estimated to be between USD 110–182 million during that period. The overall number of vendors has increased significantly since Silk Road was launched. Regarding the sales volume per vendor, the majority of vendors only made small sales volumes of less than USD 1000. Van Wegberg et al. (2018) comprehensively studied Silk Road and AlphaBay and found that commoditization on these marketplaces was spottier than previously assumed, but showed that activity and revenues on these cryptomarkets steadily increased over time. Christin (2013) showed that Silk Road's annual sales volume was around USD 15 million by mid-2012, and that most Silk Road vendors disappeared within three months of market entrance. Aldridge and Décary-Hétu (2014) found that the number of vendors and buyers using Silk Road increased, and thus its revenue increased significantly. Demant et al. (2018) estimated the total sales volume of Silk Road 2.0 and Agora to be approximately USD 66 million and USD 61 million, respectively. EUROPOL (2017a) showed that more than 100 cryptomarkets remained active for just over eight months on average.

Many studies have revealed that drugs account for a large part of the products sold on cryptomarkets. For example, both Christin (2013) and Soska and Christin (2015) found that most of the listed products are narcotics or controlled substances, and cannabis was likely to be the most popular traded drug. Aldridge and Décary-Hétu (2014) showed that drugs accounted for 17 of the 20 largest product categories on Silk Road. Broséus et al. (2016) examined illicit drug trafficking, including the number of vendors and listings, on eight marketplaces, including Agora, Evolution, and Silk Road 2.0, from a Canadian perspective. Rhumorbarbe et al. (2016) examined the number of vendors and drug listings on Evolution. Broséus et al. (2017) examined drug transactions along with information on their vendors and unit prices on Silk Road 2.0 and Evolution from an Australian perspective. Tzanetakis (2018) found that more than 60% of all sales accounted for products related to cocaine, cannabis, heroin, and ecstasy on AlphaBay.

Further, one of the first academic studies on cryptomarkets by Barratt (2012) discussed whether the market structure is business-to-business or business-to-consumer. Both Aldridge and Décary-Hétu (2016) and Barratt et al. (2016) showed that while the majority of purchases are for small amounts, most of the revenue comes from large quantities. Demant et al. (2018) showed that listed drugs on Silk Road and Agora were primarily for personal use or social networks including friends and colleagues, although a large part of the revenue was likely to come from business-to-business dealings. Décary-Hétu et al. (2016) examined vendors' risk-taking on Silk Road, and showed that willingness to ship drugs abroad was associated with several factors, including mailing weight of drug packages, vendors' reputation, and the perceived effectiveness of country-level law enforcement.

Some studies have investigated the geography of the vendors' origin countries and their accepted destination countries. Christin (2013) found that more than 40% of the countries of origin were the US and UK (around 10%), followed by the Netherlands, Canada, and Germany (between 4 and 6%). 49.7% of the listed items were available for the worldwide shipment, 35.2% for the US, around 6% for European Union and Canada, around 3% for the UK and Australia. They constitute the top countries in which cryptomarket activity has been observed (Dolliver, 2015; Norbutas, 2018; Tzanetakis, 2018). Norbutas (2018) examined the structure of the geographical trade networks of buyers and sellers of drugs on Abraxas, and found that cryptomarkets are more likely to be localized. Buyers avoid purchasing from vendors in different countries, preferring to buy from multiple vendors within a single country. Van Buskirk et al. (2016a,b) showed that the presence of vendors' origin countries on Agora was influenced by their geographical location.

Studies have also investigated the impact of policing efforts. Aldridge and Décary-Hétu (2016), Tzanetakis (2018), Barratt et al. (2016), and Bhaskar et al. (2019) examined drug sales on cryptomarkets, and indicated that they seem resilient against law enforcement and that exit scams are not likely to deter users from engaging in them. Van Buskirk et al. (2017) investigated reductions in the number of vendors across 39 cryptomarkets as a result of Operation Onymous and the closure of Evolution. They found that the disruptions were likely to temporarily impact trading at the time. However, the vendor numbers recovered at a constant rate, and it appears that these marketplaces are resilient to long-term disruption. Décary-Hétu and Giommoni (2017) showed that the impact of Operation Onymous was limited not only from the supply side—which has been extensively investigated in the literature so far—but also from the demand side. They showed that the amount of feedback from the consumption side declined when the number of vendors and listings on the supply side also declined. Van Wegberg and Verburgh (2018) examined the effect of Operation Bayonet, an international policing effort undertaken in the summer of 2017 against AlphaBay and Hansa Market, which led to the vendors' migration to a dark web marketplace called Dream Market.

There are also qualitative studies on user experiences that include motivation for the use of cryptomarkets. Van Hout and Bingham (2013) interviewed Silk Road users online and described their motives. They provided a case study of a Silk Road user. Van Buskirk et al. (2016a,b) investigated motivations of buyers in Australia and found that the main benefits of using cryptomarkets were better quality and lower cost, and that consumers tended to be of a young age. Masson and Bancroft (2018) also interviewed cryptomarket users between December 2014 and July 2017 and showed that while cryptomarkets are not restricted to the economic exchange of users, these exchanges are often accompanied by scams, hacks, and threats. Tzanetakis et al. (2016) showed that scams and fraud are likely to be widely used on cryptomarkets. Moeller et al. (2017) explored various types of theft and fraud on cryptomarkets using multiple sources, including forum posts, and revealed that cryptomarkets fall prey to hacking attempts and that the sites' administrators often abscond with users' funds. Dalins et al. (2018) showed that motivation use of cryptomarkets is more related to greed and desire rather than particular political stances when using crawling.

A few studies have examined the dark web by focusing on cryptocurrencies. The pioneering work of Meiklejohn et al. (2013) investigated Bitcoin balances held by Silk Road using records of Bitcoin transactions. Lee et al. (2019) investigated the use of cryptocurrencies on the dark web between January 2017 and March 2018. They found that Bitcoin accounted for 99.8% of the collected cryptocurrency addresses, and 80% were used for illegal purposes. They also estimated the market size to be around USD 180 million. Foley et al. (2019) investigated Bitcoin transactions between January 2009 and April 2017 to estimate illegal activity using network cluster analysis and a regression approach known as detection-controlled estimation. They showed that Bitcoin worth around USD 76 billion per year was used in cryptomarkets, and accounted for 46% of all Bitcoin transactions. Hiramoto and Tsuchiya (2020) provided sales volumes of the seven leading cryptomarkets, and how and when the leading positions changed between the marketplaces.

3. Method

This study used three heuristics proposed by Hiramoto and Tsuchiya (2020) to identify and measure activity on cryptomarkets.[3] The first heuristic is based on the way that Bitcoin transactions are recorded. The other two heuristics are based on the way that the six cryptomarkets manage their transactions with buyers and vendors. The first heuristic is briefly described using Agora addresses.[4] Fig. 1 shows how each Bitcoin transaction was recorded. Note that Bitcoin users have wallets that can contain any number of Bitcoin addresses. There are eight Bitcoin addresses[5] ($\boldsymbol{a_s}$) on the left-hand side as the input, and two Bitcoin addresses[6] ($\boldsymbol{a_r}$) on the right-hand side as the output. Fig. 1 shows a transaction between the addresses of a sender ($\boldsymbol{a_s}$) and the addresses of a receiver ($\boldsymbol{a_r}$). The former address of the output receives BTC (Bitcoin) 0.01, and the latter receives BTC 9.33. Because senders must know the private key, $sk(\boldsymbol{a_s})$, of the addresses to set the input, addresses recorded as the input in one transaction are owned by the same user (Reid and Harrigan, 2013). This is the first heuristic used to identify transactions in cryptomarkets,[7] as utilized by previous studies (Androulaki et al., 2013; Meiklejohn et al., 2013; Reid and Harrigan, 2013). It is described as follows:

> *Heuristic 1.* If more than two addresses are inputs of the same transaction, they are owned by the same user.

The other two heuristics are based on how cryptomarkets manage their transactions. To purchase illegal goods and services, users transfer their Bitcoins to the sites' Bitcoin addresses. The Bitcoins sent by users are held in escrow until the transactions are completed. After an ordered product is shipped or delivered and the marketplace takes a commission, the marketplace sends the Bitcoins to the vendor. The Bitcoin addresses owned by the cryptomarkets are likely to be publicly revealed because administrators send information of their Bitcoin addresses to users in escrow. In fact, part of the Bitcoin addresses owned by the cryptomarkets are publicly available owing to voluntary efforts. WalletExplorer[8] provides Bitcoin addresses in these marketplaces and is a useful source that has been recently used in academic research (Toyoda et al., 2018; Foley et al., 2019; Liang et al., 2019; Hiramoto and Tsuchiya, 2020). Starting from these known addresses, other unknown addresses owned by these marketplaces were searched for in the next step.

Hiramoto and Tsuchiya (2020) identified such unknown addresses by utilizing features of internal transactions among the known addresses owned by each marketplace. Examining internal Bitcoin transactions among the addresses in each marketplace shows that they sent and received BTC 0.01 to/from each other, seen in Fig. 1. Their study found that BTC 0.01 transactions accounted for around 90% of all internal transactions for all marketplaces except Evolution. Sending BTC 0.01 most likely anonymizes and secures users' transactions through the use of a tumbling service. The second heuristic is described as follows:

> *Heuristic 2.* If an address is an input (output) to a transaction that a known address of a dark web marketplace, as an output (input), receives (sends) BTC 0.01, then the input (output) address is owned by a dark web marketplace.

Based on these addresses, transactions with addresses outside of a marketplace that have such an address as an output can be traced and identified as purchases on the marketplace to further discover other unknown addresses owned. The last heuristic for identifying purchases on the marketplaces is as follows:

> *Heuristic 3.* If a transaction of an address not owned by cryptomarkets as an input has the address owned by cryptomarkets as an output, then such a transaction is identified as a purchase on these marketplaces.

The use of the three heuristics resulted in identifying more than 520,000 transactions on Silk Road during the period between June 2012 and October 2013. Over their lifetimes, there were 320,000 transactions on Silk Road 2.0; 630,000 on Agora; 260,000 on Evolution; 270,000 on Nucleus; and 130,000 on Abraxas. These heuristics are likely to identify transactions in which buyers escrow their Bitcoin to the cryptomarkets. As indicated above, the addresses identified by the three heuristics are mostly closed within themselves, so these addresses are used in escrow to send payment to other internal addresses. Therefore, it is most likely that these transactions capture the buyers' transactions in escrow.

The methodology[9] used herein has several advantages over the established method of web-scraping. It is of the upmost importance that the proposed method accurately records the times of each purchase to establish a comprehensive picture of the transactions for any frequency (e.g., hourly, daily, monthly, and the overall active period). Previous studies have examined lower frequencies of data by aggregation, and the highest frequencies that have been examined are, at most, on a weekly basis. This is because the records of Bitcoin transactions not only include the number of Bitcoins used but also the exact time in Coordinated Universal Time (UTC). UTC shows the time in a given day between 00:00 and 23:59. This

[3] See Hiramoto and Tsuchiya (2020) for details.
[4] *15MyZHa2nP5Sc3A9jWqBysVQyHhgKhYNuL* is obtained from WalletExplorer (last accessed September 6, 2020).
[5] *15MyZHa2nP5Sc3A9jWqBysVQyHhgKhYNuL* through *1L7oBRiyWKsmhmottJEyQ61hhjkuiVW5um*.
[6] *1L4dbX4optayBemAZfr75iG6aaUqmQWeky* and *197h9kuvFrW7HsR2KkzsJRX9xJNuHjnjSm*.
[7] There could be transactions that violate this heuristic resulting from Multi-signature, although it is of minor importance. Multisignature requires more than one secret key.
[8] See https://www.walletexplorer.com/(last accessed September 17, 2019).
[9] See Hiramoto and Tsuchiya (2020) for details, including its limitations.

allows identification of when buyers escrow their Bitcoins for payment and their subsequent purchases on the marketplaces. Purchases on the marketplaces can be any time after an escrow; however, it is likely that buyers make purchases promptly (within a few hours at most). Studies (e.g., Masson and Bancroft, 2018; Tzanetakis et al., 2016; Moeller et al., 2017) have shown that users are concerned about being scammed and about financial losses due to the high volatility in Bitcoin prices. For example, Aldridge and Askew (2017) provided evidence that users trust no one on cryptomarkets. Greenberg (2013) discussed Sheep's USD 6 million exit scam in 2013, and Woolf, analyzed Evolution's USD 12 million scam in March 2015. Thus, buyers are not likely to hold Bitcoin in escrow for days.

European countries including Germany and the Netherlands have between a +1 and + 2 h time zone difference from the UK, while Canada and the US have between a −5 and −8 h time zone difference. Australia has a time zone difference of between +8 and + 10 h. For example, UTC 12 indicates that it is at noon in the UK, between 1 p.m. and 2 p.m. in European countries, between 4 a.m. and 7 a.m. in Canada and the US, and between 8 p.m. and 10

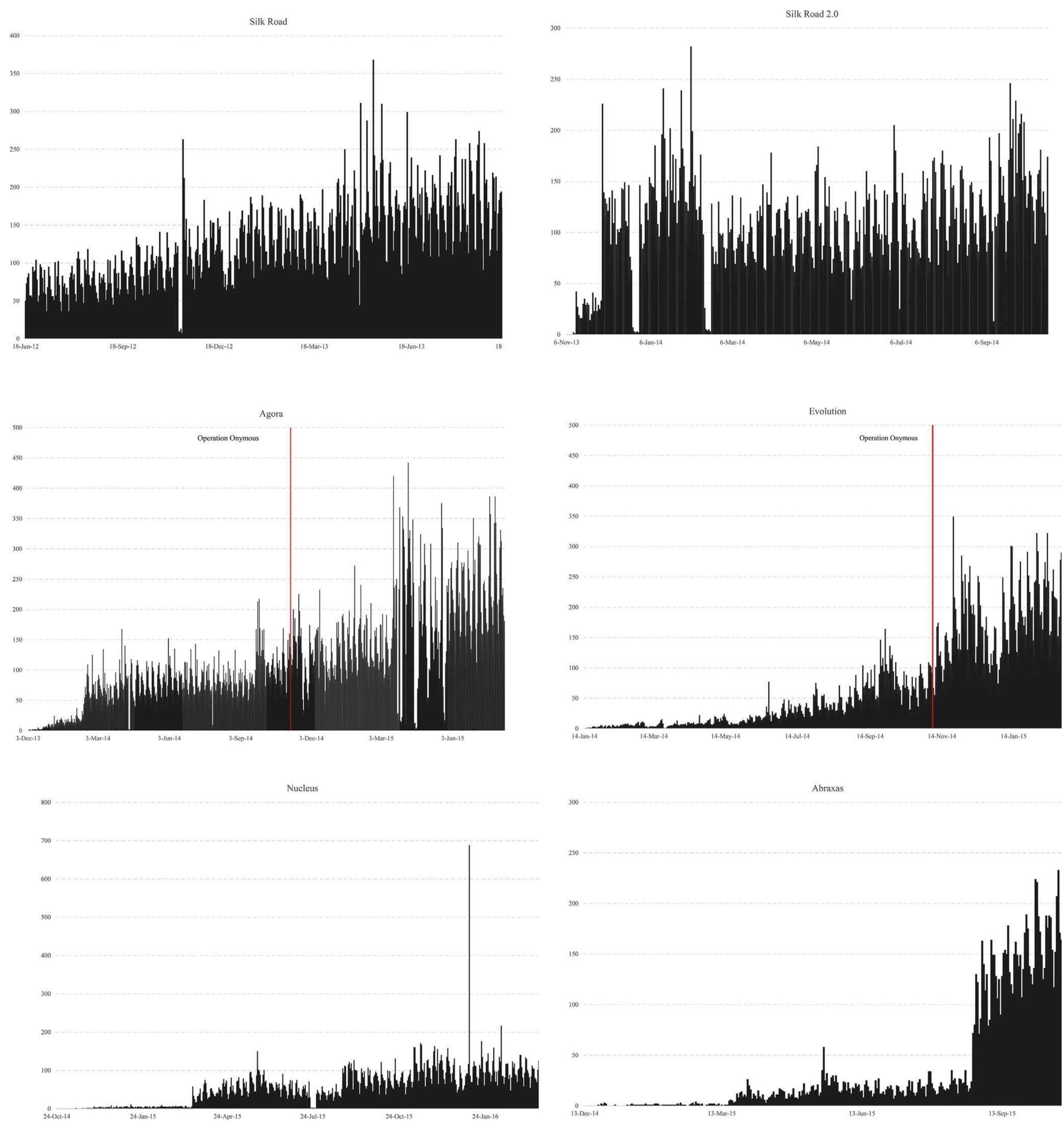


Fig. 2. Time series of hourly transaction volumes.

Table 2
Descriptive statistics: Transaction volumes.

Marketplace	Hourly					Daily					Weekly				
	Mean	Median	St. dev.	Max.	Min.	Mean	Median	St. dev.	Max.	Min.	Mean	Median	St. dev.	Max.	Min.
Silk Road	69.2	61	41.9	368	0	1660	1521	727.9	3600	70	11524	11409	4153.5	18621	5057
Silk Road 2.0	59.0	57	35.3	282	0	1415	1485	620.0	2722	0	9767	10157	3315.4	14285	5
Agora	61.5	50	54.0	442	0	1475	1292	1062.4	5550	0	10312	9200	6402.3	25900	26
Evolution	41.0	18	51.2	349	0	983	499	1087.8	4248	0	6895	3544	7372.1	22548	0
Nucleus	29.4	24	28.5	688	0	706	692	577.8	2139	0	4932	4929	3663.8	10907	0
Abraxas	22.5	5	39.3	240	0	541	136	874.1	3277	0	3699	1086	5881.0	17433	0

p.m. in Australia. Although transactions are identified in seconds, data frequency in seconds and minutes was not convenient to examine the characteristics of the occurrence of transactions. Therefore, transactions were aggregated to an hourly frequency; that is, hourly data were constructed, as it was possible to construct any frequency, including daily and weekly data.

4. Results

4.1. Development over time

Fig. 2 shows the time series of hourly transaction volumes for each marketplace. It clearly displays how the transactions for each marketplace have developed over time. The development of the hourly transaction volumes exhibits clear time series patterns, possibly resulting from the hour of day and day of week effects. Therefore, these time series characteristics were thoroughly investigated.

As has been shown in the literature (e.g., Soska and Christin, 2015; Van Wegberg and Verburgh, 2018), Fig. 2 indicates that users of such marketplaces simply migrated to other marketplaces when the leading marketplaces were no longer available. While Silk Road grew steadily, Silk Road 2.0 grew rapidly after the original Silk Road was shut down. Agora steadily increased its transactions until they were exceeded by those on Evolution at around the end of December 2014. The transactions on Evolution were small early on. The presence of Evolution sharply increased in 2014 and was in the leading position until February 2015. The rapid growth of Evolution can be attributed to Operation Onymous, through which many cryptomarkets were shut down. Users appeared to move to Evolution, which was a relatively small marketplace at that time. The transactions on Agora did not increase much for several months after Operation Onymous, probably because it was already a large marketplace and its participants were afraid of being arrested. However, after Evolution's exit scam in March 2015, Agora regained the leading position and the transactions there started to increase again, as Evolution's users appeared to migrate to Agora. Nucleus grew rapidly after Evolution's exit scam. Abraxas' transactions increased sharply in September 2015 and took the leading position until its exit scam.

However, there are two remarks pertaining to these findings. First, there were some irregular declines in the time series. This is likely to be due to the accidental downtimes of cryptomarkets (Soska and Christin, 2015; Ladegaard, 2019). Second, the users' migration was not directly observed. There were a few addresses that appeared multiple times in a single market, as users could use different addresses to trade on cryptomarkets for anonymity. Therefore, only a few addresses appeared in one marketplace and then on others.

4.2. Descriptive statistics

Table 2 shows the descriptive statistics regarding the number of transactions for each marketplace within an hour, day, and week. In terms of mean transaction volumes, Silk Road was the most active, and Silk Road 2.0 and Agora were similar. For example, on average, Silk Road had less than 70 transactions per hour, 1660 transactions per day, and 11,524 transactions per week. These findings on hourly and daily transaction volumes provide new insights into how active these cryptomarkets were, which previous studies that used lower frequency data did not reveal. The maximum transaction volumes on Agora and Evolution were much larger than on Silk Road and Silk Road 2.0, regardless of frequency. This indicates that they were more active than Silk Road when they were at their peak, suggesting that they experienced significant and rapid growth. The standard deviations of Agora and Evolution were also observed to be larger than those for Silk Road and Silk Road 2.0.

4.3. Hour of day and day of week analysis

As shown in Fig. 2, the hour-of-day and day-of-week analyses reveal the characteristics of the transactions. Fig. 3 shows heatmaps that examine the specific hour-of-day and day-of-week transaction patterns. Fig. 3 shows that there are roughly two peaks between UTC 0 and 2 and UTC 18 and 22 for the hour of day. According to previous studies, there are many illicit drug transactions on cryptomarkets in the US and European countries. This indicates that these two transaction volume peaks are attributable to transactions in the US and European countries. It is unlikely that the transaction patterns within a day differ significantly between the US and European countries. Therefore, this indicates that transactions take place during the night in countries and regions where the illicit drugs trade on cryptomarkets is most active. For the UK and European countries, including Germany and the Netherlands, the peak transaction times are at night and midnight. For the US and Canada, the peak times are between UTC 0 and UTC 2, which correspond to 4 p.m.–6 p.m. in Pacific Time and 7 p.m.–10 p.m. in Eastern Time, respectively. For Australia, night corresponds to the second most active hours for transactions, between UTC 10 and UTC 16, which is 9 p.m. and 3 a.m. in Australia's time zones. Even though Australia has, to some extent, a large illicit drug market on cryptomarkets, shares seem to be much larger in European countries and the US.

Fig. 3 indicates that most transactions take place on Mondays, Tuesdays, and Wednesdays, and fewer transactions take place on Saturdays and Sundays. This is consistent with Ladegaard (2019), who provided evidence that the drug trade on Agora and Evolution significantly decreased on Sundays. Therefore, there are more transactions at night on Mondays through Wednesdays, while there are fewer transactions all day on Saturdays and Sundays. As suggested by Ladegaard (2019), buyers on cryptomarkets are likely to purchase drugs early in the week so as to receive them by the weekend, and users purchase drugs on the weekend and on days off. In fact, through a comprehensive study of 19 European cities, Thomas et al. (2012) found that illicit drug use increases significantly on Fridays and Saturdays. Moreover, Otterstatter et al. (2016), using daily mortality data for British Columbia, Canada, found that

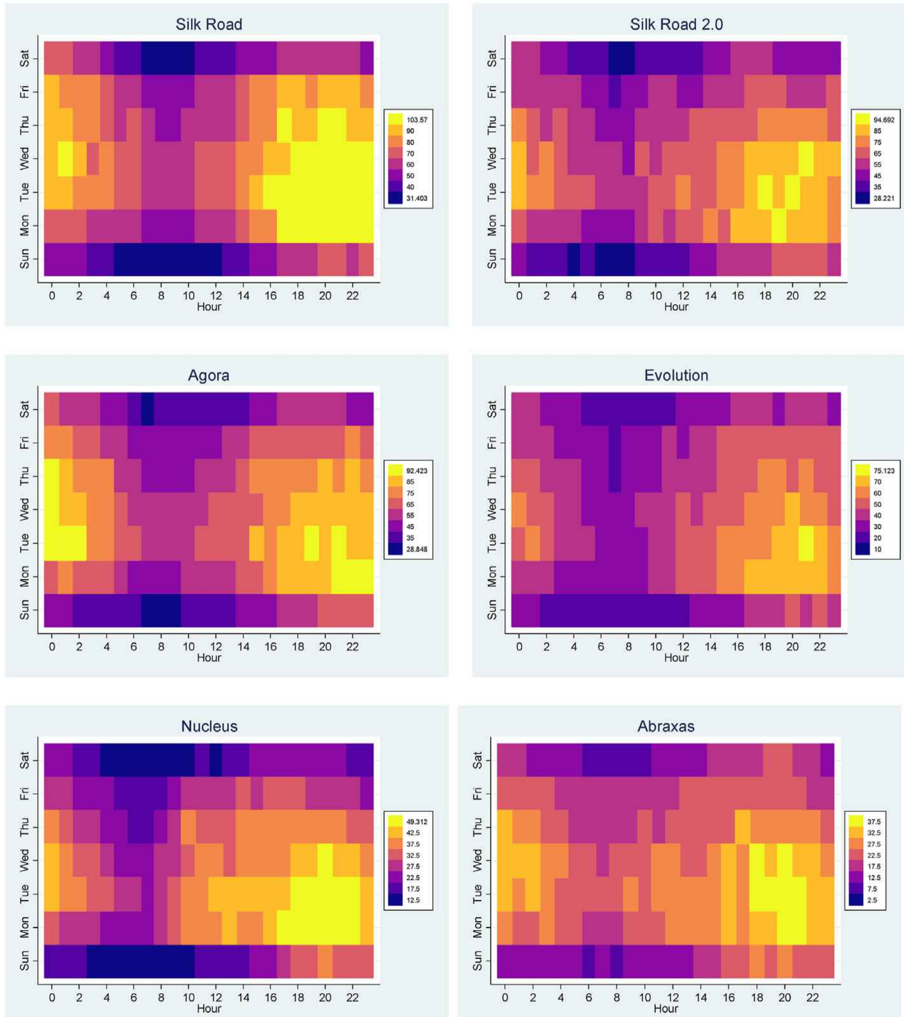


Fig. 3. Heatmap of mean transactions.

Table 3
Mean test: Transaction volumes.

Marketplace	Hour			Day of week		
	Test statistics	p-value	Observations	Test statistics	p-value	Observations
Silk Road	1535.8	(<0.001)	11328	1775.9	(<0.001)	472
Silk Road 2.0	848.4	(<0.001)	8760	1137.3	(<0.001)	365
Agora	782.2	(<0.001)	15432	1001.3	(<0.001)	643
Evolution	517.4	(<0.001)	10200	300.3	(<0.001)	425
Nucleus	778.2	(<0.001)	12912	1212.4	(<0.001)	538
Abraxas	90.7	(<0.001)	7872	174.3	(<0.001)	328

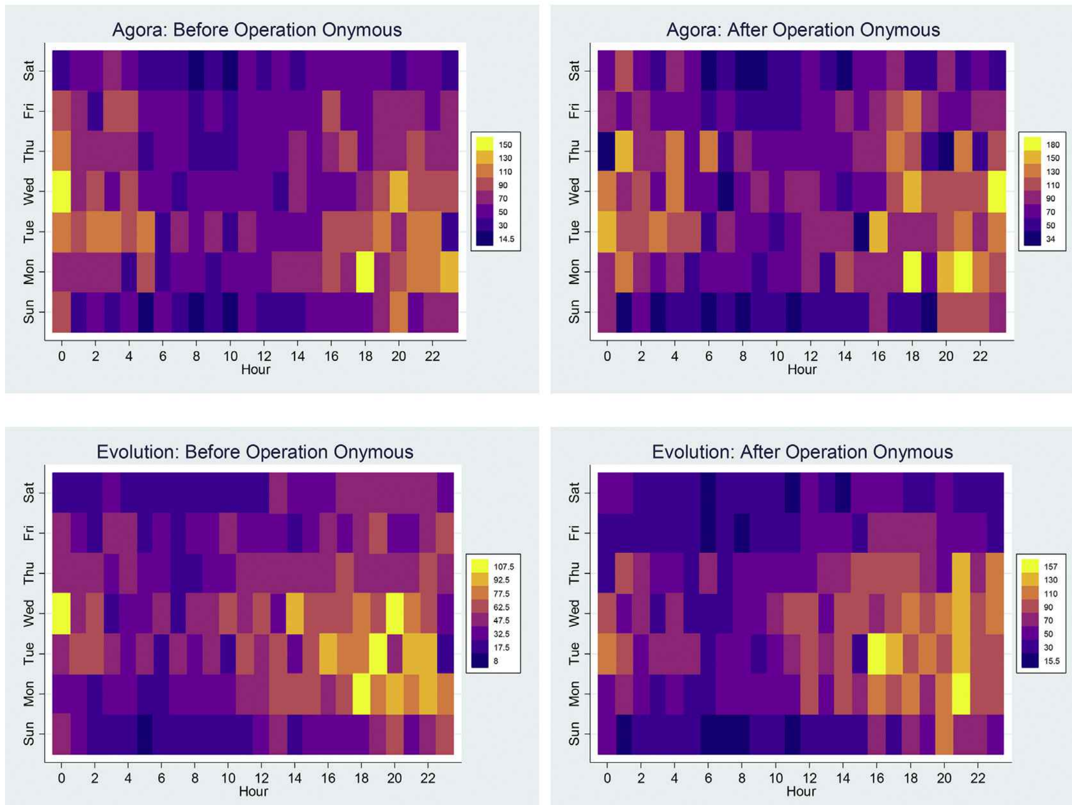
Note (<0.001) indicates that p-values are less than 0.001.

the average daily mortality rate due to overdoses on illicit drugs was above 0.8 for Saturdays and Sundays, which is higher than weekdays, whose average mortality is 0.6 at most. This indicates that drug users use drugs on their days off.

This current study's findings suggest that dark web users make drug purchases on cryptomarkets between Mondays and Wednesdays for personal use on their days off, and also suggest that products, most notably drugs, purchased on cryptomarkets are for personal use, which agrees with Aldridge and Décary-Hétu (2016), Barratt et al. (2016), and Demant et al. (2018). Further, users cannot access the dark web when they are at the office or at school, and are likely to access such sites when they return home. This finding is consistent with the considerable evidence that shows that drugs purchased on cryptomarkets are mostly for retail and not for resale or wholesale purposes. For instance, Dolliver (2015) showed that Silk Road 2.0 was not primarily a drug market between August and September 2014. This suggests that although the purpose of accessing cryptomarkets is not to purchase illicit drugs, users are cautious to avoid being seen using such sites.

To evaluate whether these patterns were accidently observed or not, Table 3 shows the results of statistical tests to evaluate the significance of the differences in the mean transaction volumes by

(A) One week before and after Operation Onymous



(B) Two weeks before and after Operation Onymous

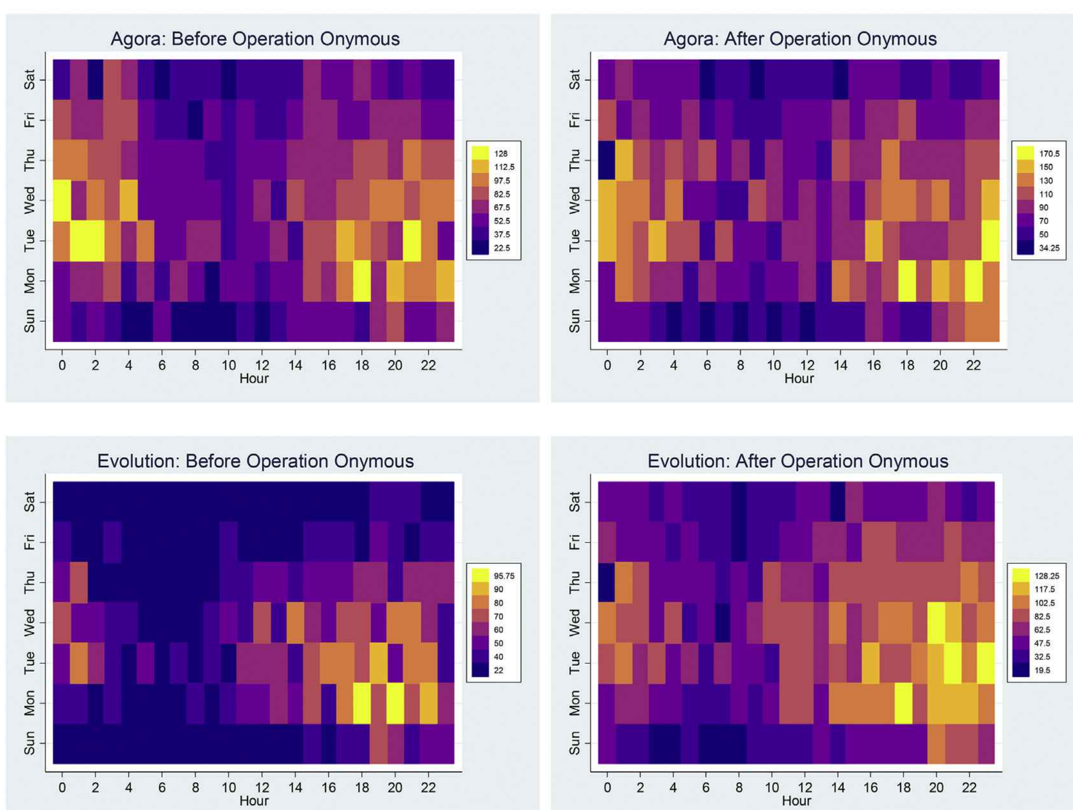


Fig. 4. Heatmap of mean transactions: Before and after Operation Onymous

(C) Four weeks before and after Operation Onymous

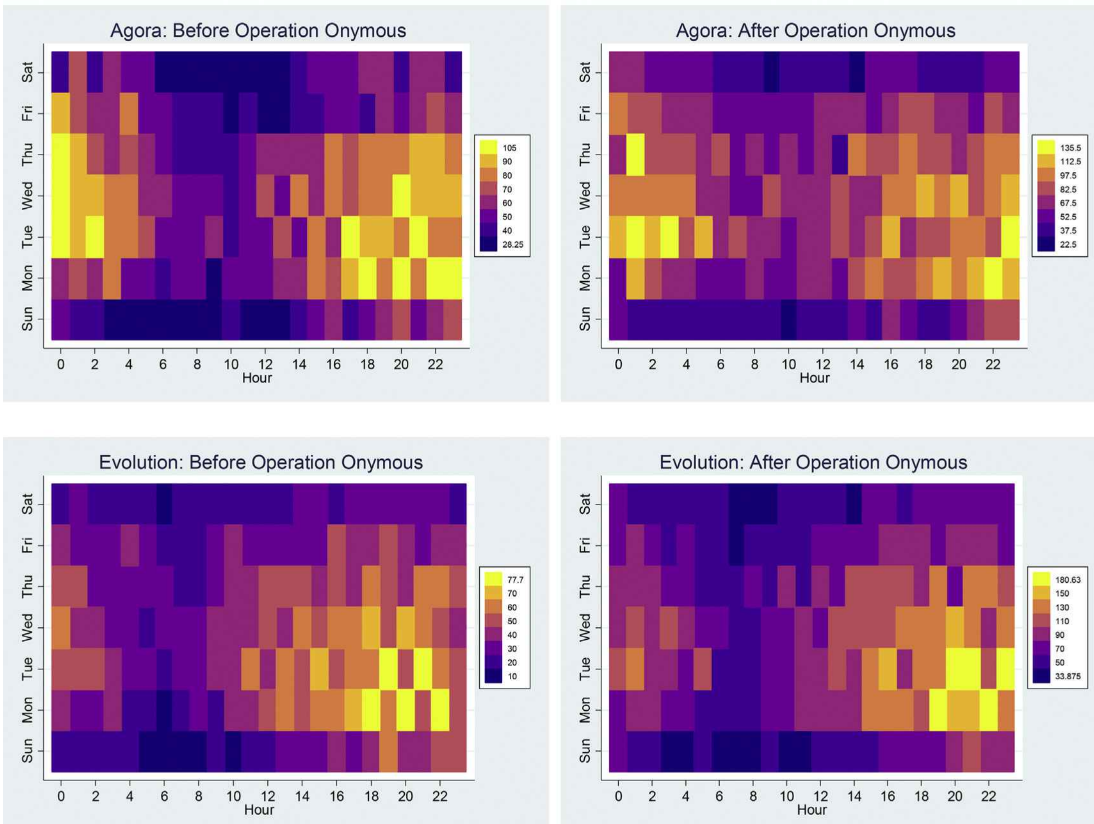


Fig. 4. (*continued*).

hour of day and day of the week, respectively. It shows that the mean transaction volumes by hour are significantly different. The null hypothesis of the equal mean is rejected at a significance level of less than 0.1% ($p < 0.001$). Similarly, the mean transaction volumes among the day of week are significantly different. The test statistics[10] were given by the likelihood-ratio test for equal means.

Although the observed transaction patterns are statistically significant, this study's interpretation that drug users place orders early on in the week and for use on the weekend runs up against the fact that cryptomarkets are internationally grounded markets, thus geographical boundaries are not likely to matter. For instance, an order placed on a cryptomarket is not received in its geographical destination until it has been packaged and shipped by the vendor and then delivered, days or even weeks later. Shipping and delivery,[11] which must rely on legitimate postal services, are one of the crucial elements of the drug trade on cryptomarkets, as discussed by Aldridge and Askew (2017). To receive an ordered product at the weekend by ordering early in the week, shipping must be domestic. If an expedited service[12] is used, an international shipment can be received within three to five days if the origin country and its destination are close, for example, between the US and Canada, and within European countries. Studies have provided evidence that supports this current study's interpretation. For example, Broséus et al. (2017) showed that activity on cryptomarkets is more localized than previously thought. Although users' identities are kept secret when ordering drugs, they are exposed to the risk of arrest when receiving the ordered products. To receive the ordered drugs, any kind of postal service is inevitably used. In particular, Broséus et al. (2017) and Cunliffe et al. (2017) revealed that the Australian online illicit drug market is moderately large and domestic due to the stringent border protection. Further, Norbutas (2018) found that the buyer-seller network is highly fragmented across geographical borders. For instance, buyers might prefer sellers from one specific country for several reasons, and buyers are likely to place orders from multiple drug sellers from a single country to avoid ordering from multiple countries. This is especially strong for continental boundaries; that is, buyers are more likely to simultaneously order drugs from sellers from several European countries than from sellers on different continents. For example, large quantities of cannabis and an especially large scale production of MDMA are produced in the Netherlands (European Monitoring Centre for Drugs and Drug Addiction, 2013), and it is likely that a significant part of these listings are for consumption within the Eurozone and elsewhere (Aldridge and Décary-Hétu, 2016; Décary-Hétu et al., 2016).

Buyers might be more willing to order domestically to avoid the increased risks of package interception, the possibility of being arrested, and long shipping times. As Hiramoto and Tsuchiya (2020)

[10] Due to the large volatility in hourly data, heterogeneous covariance was allowed instead of assuming equal covariance. See Mardia et al. (1979) and Seber (2009) for details.

[11] See, for example, Martin (2014), Tzanetakis et al. (2016), and Interpol (2015) for more detailed discussion on shipping and delivery issues.

[12] Some cryptomarkets display the availability of an expedited shipment for listed products from vendors.

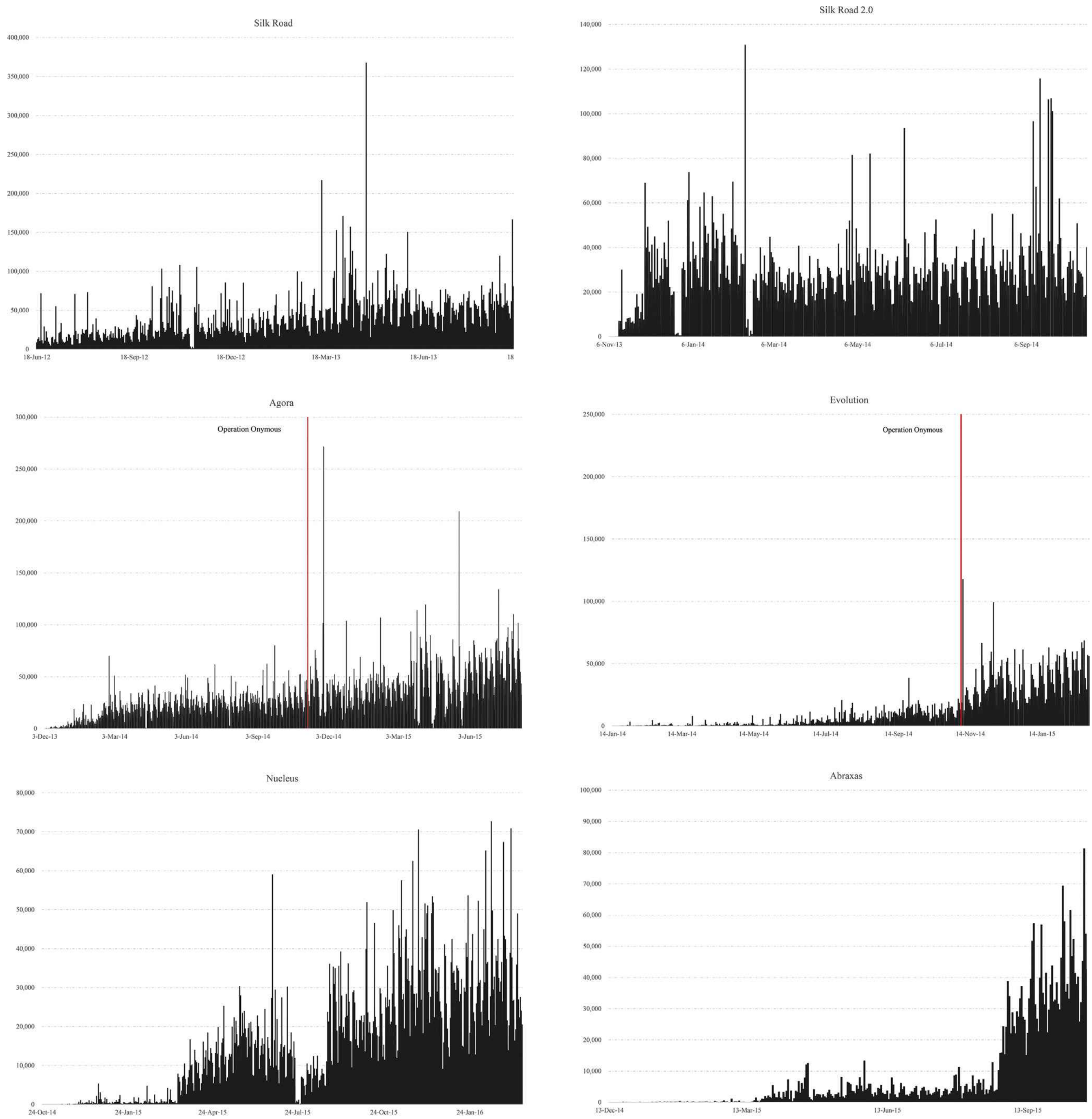


Fig. 5. Time series of hourly purchase volumes in USD.

found that average purchase prices are likely to increase over time on relatively new cryptomarkets, vendors face more risks and prices are likely to be higher. Therefore, buyers are likely to purchase illicit drugs domestically from sellers who only ship domestically because it is cheaper. Décary-Hétu et al. (2016) provided evidence that vendors ship small quantities to reduce the risk of interception, and found that one of the factors that predicted vendor willingness to risk shipping drugs across international borders was lower weight deals.

This finding also contributes to the discussion on the international nature of cryptomarkets raised by Décary-Hétu et al. (2016). Based on the cryptomarkets' transaction patterns, it may be more fruitful to investigate cryptomarkets as regional sub-markets rather than as one large international market. While the threat of law enforcement undeniably plays a significant role in increasing the risk of international shipping, the relatively high clustering of European sellers and low frequency of intercontinental trade by the same buyers might suggest that other factors, such as consideration of shipping speeds, could play a sufficient role in localizing cryptomarket exchanges. This current study's findings suggest that for monitoring and enforcement coordination purposes, data on buyers' behavior is crucial to capture the scope and potential

Table 4
Descriptive statistics: Purchase volumes.

Marketplace	Hourly					Daily					Weekly				
	Mean	Median	St. dev.	Max.	Min.	Mean	Median	St. dev.	Max.	Min.	Mean	Median	St. dev.	Max.	Min.
Silk Road	17015.0	12847.1	15440.8	367706.7	0	408360.3	337841	245430.0	1426490.3	7058.4	2834724	2750561	1385953.7	5174790	808164.8
Silk Road 2.0	12879.8	11562.6	9393.8	130766.6	0	309114.3	322693	148279.2	669783.1	0	2134506	2252534	699172.7	3218835.3	2.7
Agora	14345.0	10646.2	14449.9	271559.4	0	344280.5	307907	259710.1	1386661.5	0	2406296	2214251	1506668.8	6191590.5	3803.7
Evolution	6640.3	1512.0	10679.0	117664.7	0	159368.3	47191	219002.5	988960.4	0	1123824	334314	1449058.7	4829150	0
Nucleus	6842.8	4334.6	7982.9	72653.3	0	164228.4	133018	155986.3	627385.0	0	1147540	959802	969470.0	3008082.8	0
Abraxas	4517.2	491.4	9050.2	95002.0	0	108412.0	18805	193877.4	859814.7	0	741087	156891	1279103.8	3916376	0

growth of cryptomarkets as an international phenomenon. Therefore, this current study's findings provide evidence to support the fact that more dark web activity relating to physical products is conducted domestically than previously assumed.

The legal context is another factor that can affect domestic shipments. For example, Van Buskirk et al. (2016a,b) discussed how the prominence of cannabis listings on Agora could account for the changing political and legislative framework within the US, with some states completely legalizing cannabis, while other states have progressively decriminalized cannabis possession and consumption or legalized it for medicinal purposes. Hence, the penalty for selling and buying cannabis and cannabis-related products on cryptomarkets may be negligible depending on the source of origin and the destination within the US (Hall and Weier, 2015). Jardine and Lindner (2020) reported evidence that interest in cryptomarkets is associated with increased cannabis use in the US between 2011 and 2015, and its effect is concentrated in states with more frequent cannabis users and in states with recreational legalization of cannabis.

4.4. Impact of Operation Onymous

Operation Onymous[13] took place on November 6, 2014, and was conducted by the FBI and EUROPOL (EUROPOL, 2017b). This study investigated the impact of Operation Onymous by comparing transactions before and after the operation. Three periods before and after the operation were used: one week, two weeks, and four weeks. Fig. 1 indicated that the transaction volume did not seem to decrease soon after the operation, and there were limited impacts on the overall transactions. However, in relative terms, the transaction volume can differ from the observed pattern and provide implications for user migration.

Fig. 4 shows heatmaps of the mean transactions before and after the operation, indicating that the pattern for the entire period was observed, regardless of the cryptomarket or duration of one to four weeks. The transaction volumes increased, regardless of the hour or day of week, implying that there were virtually no impacts of Operation Onymous on Agora and Evolution, even in one week. The literature has found that the impact of police operations are limited, as cryptomarket activity recovers very quickly (Soska and Christin, 2015). Moreover, Décary-Hétu and Giommoni (2017) showed that the number of active dealers recovered to almost the pre-operation level within a month.

In contrast to this temporary effect on the supply side, this current study found no evidence of policing impact on the demand side. Décary-Hétu and Giommoni (2017), the only study that has focused on the demand side, found that the number of sales two months after Operation Onymous appeared to be twice as high as before. Sales (measured by feedback) vastly increased in the months that followed Operation Onymous. This current study further reveals that there were no policing impacts within one week, suggesting that policing operations have less impact on buyers than sellers. However, this is not distinguishable from Agora and Evolution's continuous increase soon after Operation Onymous from both the media effect of increased awareness and user migration from other cryptomarkets that had been seized. News and media reports were released immediately after the seizures, and as this information triggered public attention, new buyers and vendors were likely to flow into cryptomarkets. It is also likely that the increase in the transaction volumes on Agora and Evolution may be attributed to buyer migration from Silk Road 2.0 and other seized markets, as shown in Hiramoto and Tsuchiya's (2020) study.

[13] See EUROPOL (2014) for details.

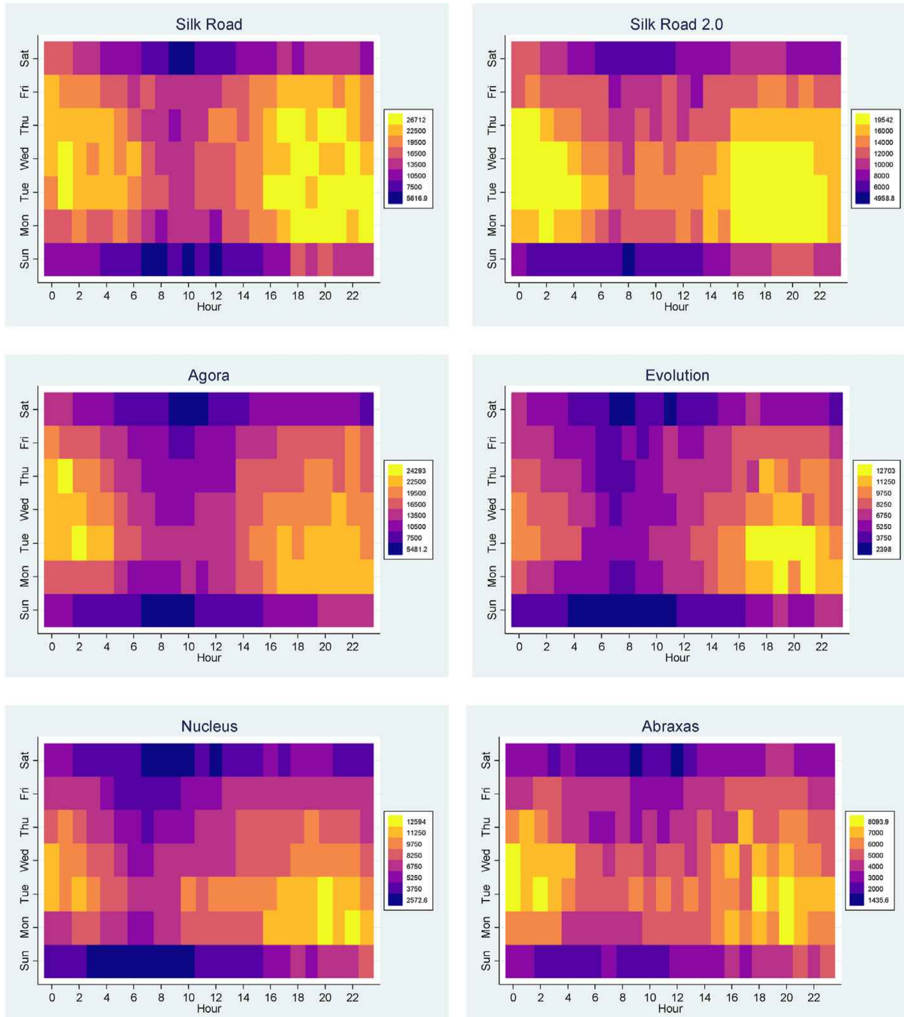


Fig. 6. Heatmap of mean purchase volumes.

Table 5
Mean test: Purchase volumes.

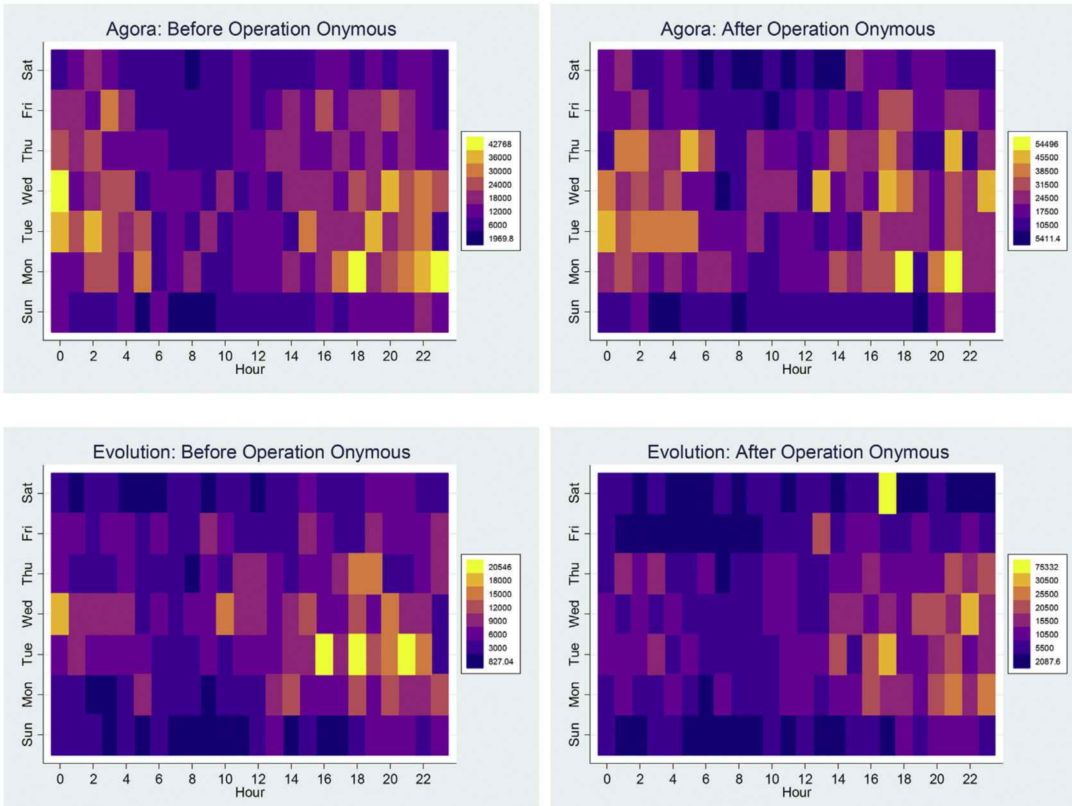
Marketplace	Hour			Day of week		
	Test statistics	p-value	Observations	Test statistics	p-value	Observations
Silk Road	809.9	(<0.001)	11328	1528.5	(<0.001)	472
Silk Road 2.0	515.4	(<0.001)	8760	1431.9	(<0.001)	365
Agora	956.2	(<0.001)	15432	371.1	(<0.001)	643
Evolution	353.3	(<0.001)	10200	1107.1	(<0.001)	425
Nucleus	400.7	(<0.001)	12912	201.2	(<0.001)	538
Abraxas	67.7	(<0.001)	7872	0.0	(<0.001)	328

Note (<0.001) indicates that p-values are less than 0.001.

However, part of these increases can be attributed to new buyers as a result of the media attention. Soon after Operation Onymous, the number of vendors decreased; thus, buyers on cryptomarkets may adapt to a police crackdown by concentrating their transactions to fewer but more trusted sellers. Due to the decreased number of sellers and higher risks, drug prices should increase if a considerable number of new buyers participate. However, Décary-Hétu and Giommoni (2017) showed that there was no evidence that prices increased after Operation Onymous. This suggests that there was no significant inflow of new buyers, and migrated users that may have trusted sellers relocated from the seized markets, accounting for a large part of the increase.

At the time of Operation Onymous, the largest alternative Silk Road 2.0 marketplaces were Agora and Evolution. Agora was the leading market, and Evolution was in second place. Wholesalers were likely to quickly migrate to Evolution from Agora. Due to Agora's large presence, wholesalers were cautious about being shut down. Another concern of Agora's users was that the marketplace had more downtime where users could not gain access (Ladegaard, 2019). Buyers and vendors review information on cryptomarkets and their new locations from various forums to avoid risk and enjoy higher privacy levels and secure trading. Evolution seems to have had a lower possibility of being seized than Agora due to its smaller size. This suggests that there was a

(A) One week before and after Operation Onymous



(B) Two weeks before and after Operation Onymous

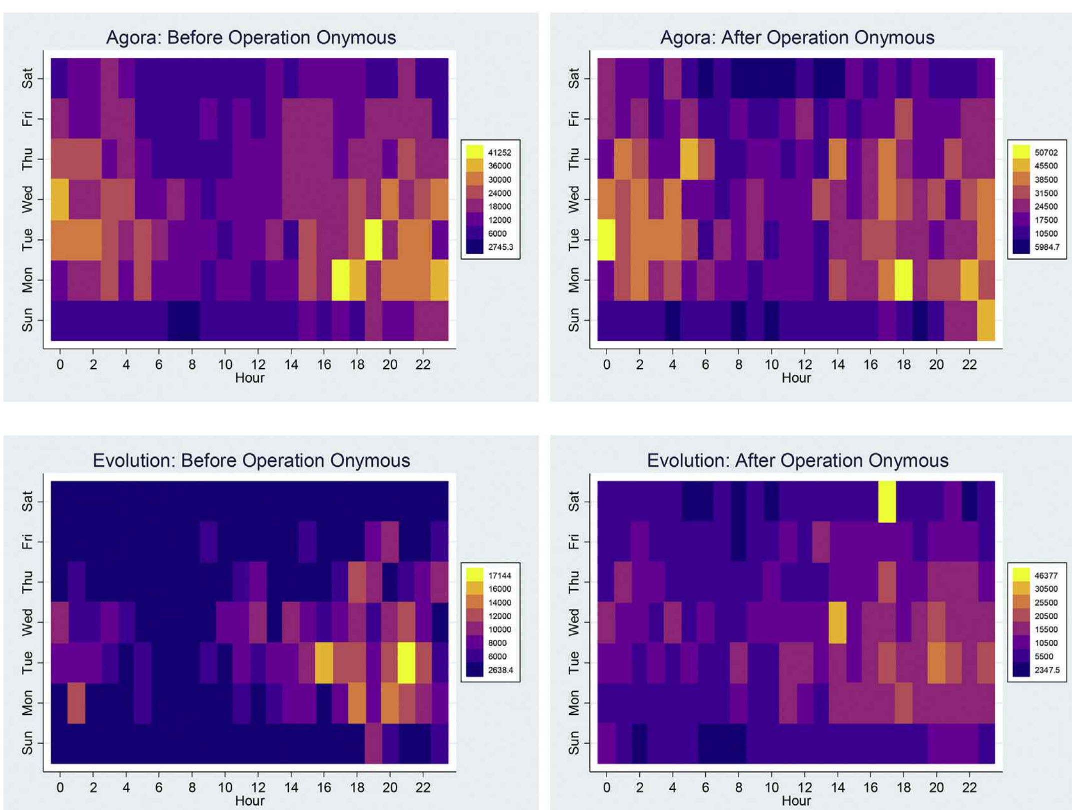


Fig. 7. Heatmap of mean purchase volumes: Before and after Operation Onymous

(C) Four weeks before and after Operation Onymous

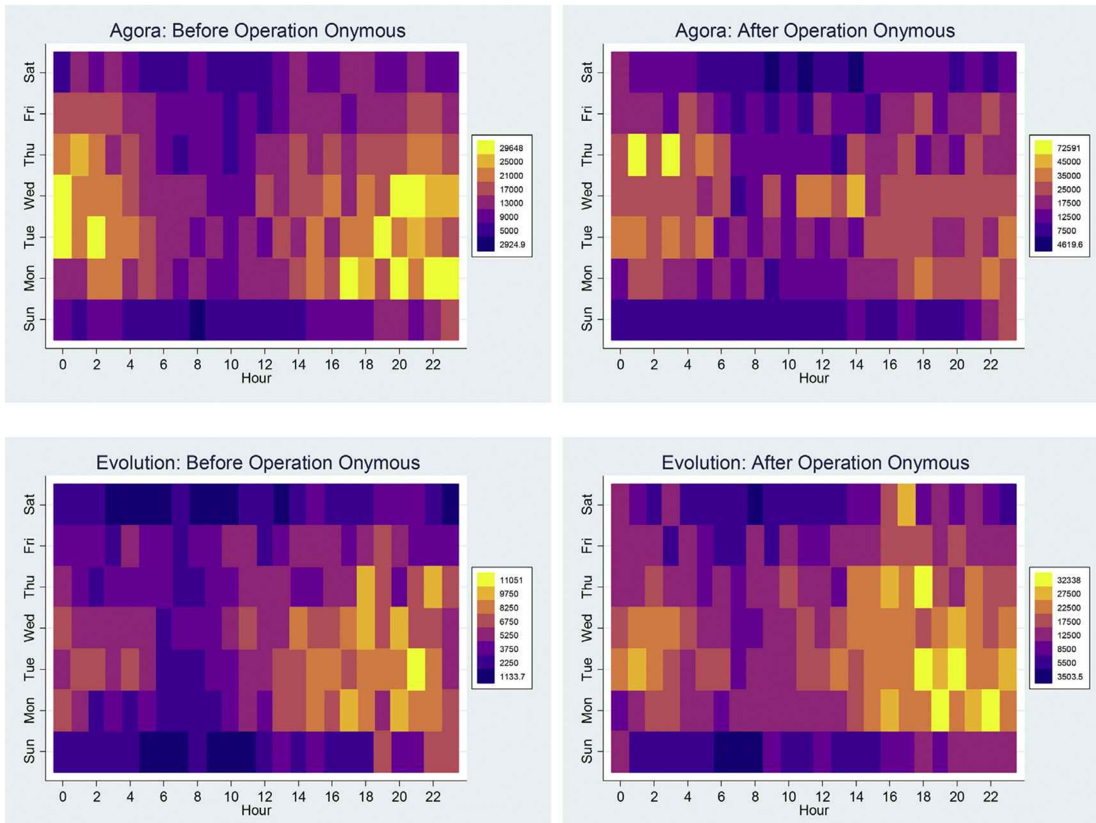


Fig. 7. (*continued*).

large user migration from Agora to Evolution. In fact, Evolution took the leading position over Agora among the cryptomarkets about a month after Operation Onymous.

A typical pattern of the lifetime of a cryptomarket is summarized as follows. After establishment, it remains a small marketplace where only small amounts of transactions are traded. For a while, there are no significant changes, or a little growth at most. It then rapidly grows due to the shutdown of other major cryptomarkets. Finally, it is seized or exits.

4.5. Robustness: purchase volume

To examine the robustness of the results, the same analysis was conducted using purchase volumes. The reasons for purchase among buyers may differ for the quantities purchased per transaction. As wholesalers may purchase large quantities per order, their purchase volumes may be larger than those of retailers. This results in a different pattern by the hour of day and day of week, given the differences in not only purchase quantities but also purchase timing between wholesalers and retailers. Another possibility that causes different patterns is the unit price. If wholesalers are more willing to order international shipping, the unit price is likely to be higher due to the larger risk for vendors. In offline dealings, the risks taken by drug sellers—of which arrest is but one—are thought to increase the prices of illegal drugs (Reuter and Kleiman, 1986), with sellers effectively compensating their acceptance of the risks by setting higher prices. To calculate the sales volume for each transaction in terms of USD, the end-of-day Bitcoin price on the date of transaction was used. Aggregating all transactions within a given hour and multiplying them by the end-of-day Bitcoin price provided the hourly sales volume for each marketplace. Daily and weekly sales volumes were calculated by aggregating the daily sales volumes within a given day and week, respectively.

Fig. 5 shows the time series of the hourly purchase volumes for each marketplace, and shows a consistent picture of how each marketplace has developed over time. Hourly purchase volumes also show clear time series patterns. Table 4 shows the corresponding descriptive statistics regarding the purchase volumes for each marketplace. The descriptive statistics provide consistent results with those of the transaction volumes,[14] indicating that the popularity of the marketplaces does not differ between the sales volumes and transaction volumes.

Fig. 6 shows heatmaps of the mean purchase volumes, and indicates that the hour-of-day and day-of-week patterns are consistent with those of the transaction volumes. This suggests that the sellers of drugs for wholesale use are likely to divide their large volumes of purchases into smaller quantities, or divide their

[14] See Hiramoto and Tsuchiya (2020) for results and a discussion on the average expenditure per transaction. In short, the majority of average expenditures are below USD 100, which is in line with previous studies.

Bitcoins for payment into small values and send them many times. This is in line with that fact that dark web users do not tend to make large Bitcoin value transactions, as this information is publicly available, may gain attention from the public, and could reveal individual identities. Table 5 shows that the mean purchase volumes by hour of day and day of week are significantly different. Fig. 7 shows heatmaps of mean purchases before and after Operation Onymous. Thus, this study can conclude that there are specific patterns in the hours and days of week on the marketplaces which are consistent with transaction volumes.

These findings show that the patterns in the purchase volumes do not differ from those of the transaction volumes, suggesting that different types of buyers (including wholesalers and retailers) place similar orders. Wholesalers are not likely to place orders of a large quantity in one transaction. This is also consistent with the literature, which has found that cryptomarket users are less willing to trade internationally. Further, avoidance of international shipping and preference for domestic dealings is likely after Operation Onymous, suggesting that the cryptomarket ecosystem develops to avoid risk exposure.

5. Discussion and limitations

This section discusses the implications of this study's findings and presents the implications for monitoring and policing cryptomarkets.

Soska and Christin (2015) argued that policing efforts of cryptomarkets should be reconsidered because law enforcement seizures of individual cryptomarkets are ineffective at reducing sales across their broad ecosystem. Although international policing efforts and law enforcement agencies are becoming increasingly important, it seems that users, including buyers and vendors, simply migrate to new marketplaces when existing ones are shut down. This suggests that policing efforts that focus on buyers and vendors rather than on shutting down cryptomarkets are likely to be more effective. In particular, monitoring cryptomarket forums and intercepting domestic shipments are likely to be effective.

As Barratt et al. (2016) suggested, users switch to personal friends or dealers to access drugs when cryptomarkets are unavailable. By displacing cryptomarket activity with conventional drug dealing, market-related harm including violence experienced by drug market participants will likely increase. Similarly, the seizure of such marketplaces along with the arrest of administrators by law enforcement authorities has not proven to be an efficient approach.

Finally, there are some limitations of this study. First, as it is impossible to determine product categories, it is not feasible to reveal which products were being purchased. This study relies on the fact that cryptomarkets mostly account for the drug trade and thus discusses the implications for drug trading. Second, the timing can differ from the actual point of purchase time. For instance, the time that buyers escrow their Bitcoins to the addresses owned by the cryptomarkets can be different from the time that they actually make a purchase. After an escrow, buyers in principle can make purchases anytime they want. Third, this study's findings cannot be automatically generalized to the newer marketplaces that emerged after those studied herein, as these were active until the end of 2015. The patterns and characteristics of drug buyers and users may change over time, which reflects the environments surrounding cryptomarkets that include new anonymity-enhancing technologies that are available, offline drug businesses, and political and legislative frameworks.

6. Conclusion

This study measured the timings when cryptomarket transactions took place via Bitcoin transactions. This study found that cryptomarket users make relatively more transactions at night on Mondays, Tuesdays, and Wednesdays, and fewer transactions on Saturdays and Sundays. This indicates that the drug trade for retail purposes accounts for a large part of the cryptomarkets. Further, this study indicates that the policing effort known as Operation Onymous only displaced users among these marketplaces and did not deter their activity, even in the short term. It also suggests that policing efforts to shut down cryptomarkets are not effective, and doggedly arresting buyers and vendors would be effective.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This study received financial support from the Telecommunications Advancement Foundation (Research Grant 2019).

References

Aldridge, J., Askew, R., 2017. Delivery dilemmas: how drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. Int. J. Drug Pol. 41, 101–109.
Aldridge, J., Décary-Hétu, D., 2014. Not an 'Ebay for drugs': the cryptomarket 'silk road' as a paradigm shifting criminal innovation (May 13, 2014). Available at: SSRN. https://ssrn.com/abstract=2436643. https://doi.org/10.2139/ssrn.2436643 (accessed 26 April 2019) [Online].
Aldridge, J., Décary-Hétu, D., 2016. Hidden wholesale: the drug diffusing capacity of online drug cryptomarkets. Int. J. Drug Pol. 35, 7–15.
Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S., 2013. Evaluating user privacy in bitcoin. In: International Conference on Financial Cryptography and Data Security, pp. 34–51.
Barratt, M.J., 2012. Silk road: ebay for drugs. Addiction 107 (3), 683-683.
Barratt, M.J., Ferris, J.A., Winstock, A.R., 2016. Safer scoring? Cryptomarkets, social supply and drug market violence. Int. J. Drug Pol. 35, 24–31.
Bhaskar, V., Linacre, R., Machin, S., 2019. The economic functioning of online drugs markets. J. Econ. Behav. Organ. 159, 426–441.
Broséus, J., Morelato, M., Tahtouh, M., Roux, C., 2017. Forensic drug intelligence and the rise of cryptomarkets. Part i: studying the australian virtual market. Forensic Sci. Int. 279, 288–301.
Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., Décary-Hétu, D., 2016. Studying illicit drug trafficking on darknet markets: structure and organisation from a canadian perspective. Forensic Sci. Int. 264, 7–14.
Christin, N., 2013. Traveling the silk road: a measurement analysis of a large anonymous online marketplace. In: Proceedings of the 22nd International Conference on World Wide Web, pp. 213–224.
Cunliffe, J., Martin, J., Décary-Hétu, D., Aldridge, J., 2017. An island apart? Risks and prices in the australian cryptomarket drug trade. Int. J. Drug Pol. 50, 64–73.
Dalins, J., Wilson, C., Carman, M., 2018. Criminal motivation on the dark web: a categorisation model for law enforcement. Digit. Invest. 24, 62–71.
Décary-Hétu, D., Giommoni, L., 2017. Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation onymous. Crime Law Soc. Change 67 (1), 55–75.
Décary-Hétu, D., Paquet-Clouston, M., Aldridge, J., 2016. Going international? Risk taking by cryptomarket drug vendors. Int. J. Drug Pol. 35, 69–76.
Demant, J., Munksgaard, R., Houborg, E., 2018. Personal use, social supply or redistribution? Cryptomarket demand on silk road 2 and agora. Trends Organ. Crime 21 (1), 42–61.
Dingledine, R., Mathewson, N., Syverson, P., 2004. Tor: the Second-Generation Onion Router. Naval Research Lab, Washington DC.
Dolliver, D.S., 2015. Evaluating drug trafficking on the tor network: silk road 2, the sequel. Int. J. Drug Pol. 26 (11), 1113–1123.
European Monitoring Centre for Drugs and Drug Addiction, 2013. EU Drug Markets Report: A Strategic Analysis. Publications Office of the European Union.
Europol, 2014. Global action against dark markets on tor network. https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network (accessed 6 May 2019) [Online].
Europol, 2017a. Drugs and the darknet: perspectives for enforcement, research and policy. https://www.europol.europa.eu/publications-documents/drugs-and-

darknet-perspectives-for-enforcement-research-and-policy (accessed 6 May 2019) [Online].
Europol, 2017b. Massive blow to criminal dark web activities after globally coordinated operation. https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation (accessed 6 May 2019) [Online].
Foley, S., Karlsen, J.R., Putniņš, T.J., 2019. Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies? Rev. Financ. Stud. 32 (5), 1798–1853.
Greenberg, A., 2013. Silk road competitor shuts down and another plans to go offline after claimed $6 million theft. https://www.forbes.com/sites/andygreenberg/2013/12/01/silk-road-competitor-shuts-down-and-another-plans-to-go-offline-after-6-million-theft/#1388af767e08 (1 December 2013) (accessed 2 August 2020) [Online].
Hall, W., Weier, M., 2015. Assessing the public health impacts of legalizing recreational cannabis use in the USA. Clin. Pharmacol. Ther. 97 (6), 607–615.
Hiramoto, N., Tsuchiya, Y., 2020. Measuring dark web marketplaces via bitcoin transactions: from birth to independence. Forensic Sci. Int.: Digit. Invest. 35, 301086.
Interpol, 2015. Pharmaceutical crime on the darknet. A study of illicit online marketplace. https://www.gwern.net/docs/sr/2015-interpol-pharmaceuticals.pdf (accessed September 1 2020) [Online].
Jardine, E., Lindner, A.M., 2020. The dark web and cannabis use in the United States: evidence from a big data research design. Int. J. Drug Pol. 76, 102627.
Ladegaard, I., 2019. Crime displacement in digital drug markets. Int. J. Drug Pol. 63, 113–121.
Lee, S., Yoon, C., Kang, H., Kim, Y., Kim, Y., Han, D., Son, S., Shin, S., 2019. Cybercriminal minds: an investigative study of cryptocurrency abuses in the dark web. In: Network and Distributed Systems Security (NDSS) Symposium 2019.
Liang, J., Li, L., Luan, S., Gan, L., Zeng, D., 2019. Bitcoin exchange addresses identification and its application in online drug trading regulation. In: Pacific Asia Conference on Information Systems (PACIS 2019).
Mardia, K., Kent, J., Bibby, J., 1979. Multivariate Analysis. Academic Press Inc, London.
Martin, J., 2014. Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs. Springer.
Masson, K., Bancroft, A., 2018. 'Nice people doing shady things': drugs and the morality of exchange in the darknet cryptomarkets. Int. J. Drug Pol. 58, 78–84.
Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., Mccoy, D., Voelker, G.M., Savage, S., 2013. A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement Conference, pp. 127–140.
Moeller, K., Munksgaard, R., Demant, J., 2017. Flow my FE the vendor said: exploring violent and fraudulent resource exchanges on cryptomarkets for illicit drugs. Am. Behav. Sci. 61 (11), 1427–1450.
Nakamoto, S., 2008. Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf (Accessed 20 March 2019) [Online].
Norbutas, L., 2018. Offline constraints in online drug marketplaces: an exploratory analysis of a cryptomarket trade network. Int. J. Drug Pol. 56, 92–100.
Otterstatter, M.C., Amlani, A., Guan, T.H., Richardson, L., Buxton, J.A., 2016. Illicit drug overdose deaths resulting from income assistance payments: analysis of the 'check effect'using daily mortality data. Int. J. Drug Pol. 33, 83–87.
Reid, F., Harrigan, M., 2013. An analysis of anonymity in the bitcoin system. In: Security and Privacy in Social Networks. Springer, pp. 197–223.
Reuter, P., Kleiman, M.A., 1986. Risks and prices: an economic analysis of drug enforcement. Crime Justice 7, 289–340.
Rhumorbarbe, D., Staehli, L., Broséus, J., Rossy, Q., Esseiva, P., 2016. Buying drugs on a darknet market: a better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data. Forensic Sci. Int. 267, 173–182.
Seber, G.A., 2009. Multivariate Observations. John Wiley & Sons.
Soska, K., Christin, N., 2015. Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In: 24th USENIX Security Symposium (USENIX Security 15), pp. 33–48.
Thomas, K.V., Bijlsma, L., Castiglioni, S., Covaci, A., Emke, E., Grabic, R., Hernández, F., Karolak, S., Kasprzyk-Hordern, B., Lindberg, R.H., Lopez De Alda, M., Meierjohann, A., Ort, C., Pico, Y., Quintana, J.B., Reid, M., Rieckermann, J., Terzic, S., Van Nuijs, A.L.N., De Voogt, P., 2012. Comparing illicit drug use in 19 european cities through sewage analysis. Sci. Total Environ. 432, 432–439.
Toyoda, K., Ohtsuki, T., Mathiopoulos, P.T., 2018. Multi-class bitcoin-enabled service identification based on transaction history summarization. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp. 1153–1160.
Tzanetakis, M., 2018. Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. Int. J. Drug Pol. 56, 176–186.
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. Int. J. Drug Pol. 35, 58–68.
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 Alcohol Depend. 173, 159–162.
Van Buskirk, J., Naicker, S., Roxburgh, A., Bruno, R., Burns, L., 2016a. Who sells what? Country specific differences in substance availability on the agora cryptomarket. Int. J. Drug Pol. 35, 16–23.
Van Buskirk, J., Roxburgh, A., Bruno, R., Naicker, S., Lenton, S., Sutherland, R., Whittaker, E., Sindicich, N., Matthews, A., Butler, K., 2016b. Characterising dark net marketplace purchasers in a sample of regular psychostimulant users. Int. J. Drug Pol. 35, 32–37.
Van Hout, M.C., Bingham, T., 2013. 'Surfing the silk road': a study of users' experiences. Int. J. Drug Pol. 24 (6), 524–529.
Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Ganan, C.H., Klievink, B., Christin, N., Van Eeten, M., 2018. Plug and prey? Measuring the commoditization of cybercrime via online anonymous markets. In: 27th USENIX Security Symposium (USENIX Security 18), pp. 1009–1026.
Van Wegberg, R., Verburgh, T., 2018. Lost in the dream? Measuring the effects of operation bayonet on vendors migrating to dream market. In: Proceedings of the Evolution of the Darknet Workshop, pp. 1–5.
Woolf, N.. Bitcoin 'exit scam': deep-web market operators disappear with $12m. https://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars (18 March 2015). (accessed July 21.2020).