Measuring dark web marketplaces via Bitcoin transactions: From birth to independence

Naoki Hiramoto a, Yoichi Tsuchiya b, *

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

ABSTRACT
This study measures the evolution of the anonymous marketplaces Silk Road, Silk Road 2.0, Agora, Evolution, Nucleus, Abraxas, and AlphaBay, which were the seven leading and most active dark web marketplaces. We identify that all the seven marketplaces use the same software to manage Bitcoin by investigating transactions in these marketplaces. However, the software was no longer used since May 2016 because of its vulnerability to protect anonymity. It indicates that dark web marketplaces advanced to the next stage with anonymity-enhancing tools around in March 2016. Using simple heuristics to identify and trace Bitcoin addresses associated with these marketplaces, purchases on these marketplaces are identified and evaluated. Our method provides evidence on market size, development, and fluctuation over time to fill a gap in previous studies. Dark web marketplaces continue to thrive because users migrate to new marketplaces after the existing ones are shut down. The total sales volume on Silk Road was 192.7 million US dollars between June 2012 and October 2013. The corresponding figures for Silk Road 2.0, Agora, Evolution, Nucleus, and Abraxas were 112.9, 220.7, 69.7, 88.3, and 35.6 million US dollars, respectively. The figures for AlphaBay was 166.0 million US dollars between December 2014 and February 2016.

1. Introduction

Technologies that ensure security and privacy are the key to promoting online activity. Although they may introduce pioneering goods and services that benefit society, they may also provide offenders with tools for illegal activity. In particular, two online anonymizing technologies have led to the creation of dark web marketplaces. The first technology is Bitcoin, which is a fully decentralized digital currency based on blockchain (Nakamoto, 2008). A public distributed ledger called blockchain is used to maintain all transaction history to prevent double spending and avoid central control. Although all transaction records are public, Bitcoin payments are anonymous unless Bitcoin addresses and transactions can be matched to actual identities in society. 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).

Thus, it is difficult to determine the locations of the visitors of a website because a website can only trace back the connection to the last relay. Administrators of sites on dark web can conceal the location of their website servers and thus avoid law enforcement agencies.

Silk Road, the first successful dark web marketplace, was launched in February 2011. Numerous dark web marketplaces have been launched since then. These new online marketplaces focus on anonymity and security to limit the risks of identification although they share many aspects of legitimate online markets such as eBay and Amazon (Christin, 2013). Although the Federal Bureau of Investigation (FBI) shut down various dark web marketplaces, the impact of police intervention is limited because of the rapid recovery of illicit transactions on dark web (Soska and Christin, 2015; Aldridge and Décault, 2016; Van Wegberg and Verburgh, 2018). Nevertheless, international policing efforts toward shutting down dark web marketplaces involving pseudo-anonymous transactions are increasingly important measures against cybercrimes.

Numerous studies have used scraping frameworks to collect data and measure activity in dark web marketplaces. This approach
results in the following types of measurement errors (Soska and Christin, 2015). First, the scraping methods may not extract all the information because scraping is not always available. Second, and more seriously, scraping cannot obtain the realized prices and quantities because the buyers’ feedback is used to indicate the quality of the vendors and their goods. Thus, the realized prices and quantities can be different from those of the listings. Furthermore, the feedback may not be timely and the scraping cannot cover the entire lifetime of a certain dark web market. Hence, the market development over time may be inaccurate.

This study is one of few studies to investigate dark web marketplaces via Bitcoin transactions thoroughly by focusing on Silk Road, Silk Road 2.0, Agora, Evolution, Nucleus, Abraxas, and AlphaBay, which were the largest and most active marketplaces operated between 2011 and 2017. The measurement errors in the established methods are avoided because the records of Bitcoin transactions provide accurate information on the sales volumes and dates of each transaction. Therefore, our approach provides evidence on market size, development, and fluctuation over time to fill a gap in previous studies. In particular, our method provides estimates for activities on marketplaces that have not been investigated. The Bitcoin balance held by Silk Road was investigated using records of Bitcoin transactions (Meiklejohn et al., 2013). By contrast, our method focuses on a feature of Bitcoin transaction management that has not been examined previously, and applies it to the seven above-mentioned marketplaces. Thus, we can determine not only the marketplace activity but also the reasons for growth and shut-down more clearly.

Using simple heuristics to measure the transactions on the seven marketplaces, we obtain the following results. We identify that all the seven marketplaces use the same software to manage Bitcoin by investigating transactions in these marketplaces. The total sales volume of Silk Road is 192.7 million USD between June 2012 and October 2013. The corresponding figures are 112.9 million USD for Silk Road 2.0, 220.7 million USD for Agora, 69.7 million USD for Evolution, 88.3 million USD for Nucleus, 35.6 million USD for Abraxas over its entire lifetime. Finally, the figure for AlphaBay is 166.0 million USD between December 2014 and February 2016. Silk Road grew steadily, and Silk Road 2.0 grew and reached its peak rapidly after the shut down of Silk Road. Agora followed Silk Road 2.0 and took the leading position around Operation Onymous. Evolution grew rapidly and overtook Agora as the leading marketplace one month after Operation Onymous. Owing to the exit scam of Evolution, Agora attained its peak sale volume and regained the leading position, while Nucleus also showed rapid growth and AlphaBay’s significant growth followed. Moreover, Nucleus, Abraxas, and AlphaBay grew further owing to the shut-down of Agora. Thus, dark web marketplaces continue to thrive because their users migrate to new marketplaces after law enforcement agencies shut down the existing ones. The majority of purchases on the seven above-mentioned dark web marketplaces are worth less than 100 USD, whereas purchases worth more than 1000 USD account only for a small percentage of the total purchases. Thus, users of dark web marketplaces buy illegal products or services for their own use and not for resale or wholesale purposes.

The remainder of this paper is organized as follows. Section 1 provides the background information on dark web marketplaces as well as a brief overview of related studies. Section 2 describes our new measurement methods for identifying transactions on dark web marketplaces and estimating their revenues. Section 3 presents the estimation results and compares their validity with the literature. Section 4 discusses the implications of the study.

2. Background and related work

2.1. Dark web

The dark web refers to World Wide Web content that requires special software and communication methods. In particular, Tor enables users to access the Internet anonymously. Hence, it is preferred by journalists, whistleblowers, and cybercriminals. Dark web marketplaces provide a new anonymous and international platform for a wide range of illicit goods and services including psychoactive substances, pornographic material, and false documents such as fake ID cards and driving licenses (Christin, 2013). Recently, stolen identities have been available for retail sale on dark web marketplaces (Steel, 2019).

Such marketplaces do not sell any product. dark web marketplaces hold Bitcoins paid by buyers in escrow and vendors are paid by the dark web marketplaces once their orders are finalized. The recent development of dark web marketplaces supported by anonymizing technologies has provided better and more sophisticated risk mitigation for participants (Soska and Christin, 2015). In fact, according to anonymous online interviews, the main reasons for accessing and using Silk Road are the site’s anonymity, wide variety of products advertised, and transaction system including vendor feedback ratings (Van Hout and Bingham, 2013). Silk Road attracted considerable attention from the media, government authorities, law enforcement agencies, and researchers before it was finally shut down after the FBI arrested its operators in early October 2013. Table 1 shows active periods of each dark web marketplace. After around a month, Silk Road 2.0, the successor to Silk Road, was launched. Subsequently, numerous marketplaces following the same business model of offering an anonymous platform for vendors and buyers emerged. However, these dark web marketplaces disappeared quickly because of voluntary closure, shut-down by law enforcement agencies, or discontinued operation after scamming vendors and buyers. EUROPOL (2017a) shows the lifetime of more than 100 dark web marketplaces that remained active for just over eight months, on average.

Among platforms with varying sizes and features, Agora, which operated between December 2013 and August 2015, and Evolution, which operated between January 2014 and March 2015, overtook Silk Road and Silk Road 2.0. Evolution grew rapidly and became the largest dark web marketplace after several dark web marketplaces including Silk Road 2.0 were shut down by an international law enforcement operation called Operation Onymous in November 2014, undertaken by the FBI and European Police Office (EUROPOL, 2017a). The law enforcement agencies seized not only Bitcoins worth approximately 1 million USD but also cash, drugs, gold, and silver worth 180,000 Euro in addition to making 17 arrests and shutting down 27 sites (EUROPOL, 2014). Although Agora and Evolution were active, they were not taken down.

Agora took the leading position after the exit scam of Evolution (EUROPOL, 2017a), and it was then closed voluntarily. AlphaBay was launched by Alexandre Cazes in December 2014. It became the largest and most popular marketplace in 2015. However, AlphaBay and Hansa Market were taken down by an internationally coordinated police operation in July 2017, and Alexandre Cazes was arrested (EUROPOL, 2017b; United States District Court, 2017). Nucleus and Abraxas were launched around the launch of AlphaBay. Nucleus operated between October 2014 and April 2016. Abraxas operated between December 2014 to November 2015. The two marketplaces grew along with a rapid growth of AlphaBay. They both exit scam.
Studies by academic scholars have provided estimates of market characteristics, including the numbers of listings, vendors, and product categories as well as sales volumes, via scraping methods. These studies have revealed several aspects of dark web marketplaces from vendor perspectives, because scraping methods collect information on feedback received by the vendors. Table 1 summarizes observed periods, estimated revenues, and the number of vendors for related works.

The most comprehensive study scraped 35 marketplaces a total of 1905 times and collected 78,509 item listings between 2013 and 2015 (Soska and Christin, 2015). The total market volume was reported to reach a peak of 650,000 USD and it remained stable at around 300,000 to 500,000 USD a day, implying that the overall annual revenue was between 110 and 182 million USD during that period. The overall number of vendors has increased significantly since Silk Road was launched; there were a total of 1400 vendors on Silk Road at the time of its shut-down. This suggests that the competition among not only vendors but also dark web marketplaces has become more intense. Regarding the sales volume per place has become more intense. Regarding the sales volume per

Table 1

<table>
<thead>
<tr>
<th>Marketplaces</th>
<th>Active periods</th>
<th>Estimates in previous studies</th>
<th>Total revenues (monthly revenues)</th>
<th>Number of vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silk Road</td>
<td>January 2011–October 2013</td>
<td>Christin (2013); February 2012–July 2012</td>
<td>Aldridge and Décarey-Hétu (2014); September 2013</td>
<td>15* (1.2) million USD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Soska and Christin (2015); November 2011–July 2012, and June 2013–August 2013</td>
<td></td>
<td>89.7* (7.5) million USD</td>
</tr>
<tr>
<td>Silk Road 2.0</td>
<td>November 2013–November 2014</td>
<td>Demant et al. (2018); February 2014–November 2014</td>
<td></td>
<td>100* (8.3) million USD</td>
</tr>
<tr>
<td>Evolution</td>
<td>January 2014–March 2015</td>
<td>Rhumorbarbe et al. (2016); January 2014–March 2015</td>
<td></td>
<td>61 (10.2) million USD</td>
</tr>
<tr>
<td>Nucleus</td>
<td>October 2014–April 2016</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abraxas</td>
<td>December 2014–November 2015</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AlphaBay</td>
<td>December 2014–July 2017</td>
<td>Christin (2017); March 2015–May 2017</td>
<td>Tzanetakis (2018); September 2015–August 2016</td>
<td>222.9 (8.3) million USD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>94 (7.8) million USD</td>
</tr>
</tbody>
</table>

Notes: Active periods are from EUROPOL (2017a, 2017b). * Annualized estimate. ** Annualized estimate of 2013.

Note that Bitcoin is not the only cryptocurrency used on dark web marketplaces. For example, Monero and Ethereum have been used on AlphaBay. Nevertheless, Bitcoin is the preferred cryptocurrency for users, and other cryptocurrencies have been used sparingly.

2.2. Related work

For Silk Road, 24,385 unique drugs listed by 1239 distinct sellers were collected and analyzed (Christin, 2013). The calculated total sales volume was 1.22 million USD per month, which corresponds to an annual sales volume of around 15 million USD by mid-2012. It was found that most Silk Road vendors disappeared within three months of market entrance and only 5% remained active for the entire sample period. Further, the number of vendors and buyers using Silk Road was found (Aldridge and Décarey-Hétu, 2014) to increase significantly and the revenue increased from a total of 14.4 million USD in mid-2012 to a total of 89.7 million USD in September 2013, which was shortly before the marketplace was shut down. The annual sales volume was shown (Soska and Christin, 2015) to increase to over 100 million USD for 2013.

Only a few studies have focused on Silk Road 2.0, Agora, Evolution, Nucleus, and Abraxas. The total sales volume of Silk Road 2.0 between 28 February 2014 and November 2014 was estimated to be approximately 66 million USD (Demant et al., 2018). For Agora, data between November 28, 2014, and April 24, 2015 was collected (Demant et al., 2018), and the total sales volume was estimated to be approximately 61 million USD. The number of vendors on Agora increased sharply until it reached its peak of more than 1000 in Fall 2014, and it then decreased to less than 1000 in January 2015 (Soska and Christin, 2015). For Evolution, a study between January 2014 and March 2015 revealed that there were 48,026 listings and 2702 vendors (Rhumorbarbe et al., 2016). The number of vendors was around 1500 in July 2014, and a sharp drop followed. Then, in contrast to Agora, it increased and exceeded 2000 in January 2015 (Soska and Christin, 2015).

For AlphaBay, data between March 18, 2015 and May 24, 2017 was collected (Christin, 2017) with 27 full scrapes, and AlphaBay was found to take the leading position toward the end of 2015. Its revenue steadily increased toward the end of the sample period, which was roughly twice as large as that of Silk Road at its peak. The estimated total revenue was around 222.9 million USD and the total worth of the transactions was around 2.2 million. Furthermore, the activity on AlphaBay between May 2015 and February 2017 was estimated (United States District Court, 2017). There were more than 4.0 million transactions conducted in Bitcoin addresses associated with AlphaBay. Thus, approximately 450 million USD were deposited with AlphaBay. The legal authorities revealed that a mixer service was introduced in April 2016 and there were more than 340,000 wallet addresses for Bitcoin. The difference might be related to the law authorities' double-counting due to currency mixing (Christin, 2017). Tzanetakis (2018) conducted data collection by focusing on drug trading between September 2015 and August 2016. The total sales volume for the drug section was estimated as 93.98 million USD for the sample period. The monthly revenues steadily increased from 0.14 million USD in September 2015 to a peak of 16.05 million USD in August 2016.
There is a recent study that investigated uses of cryptocurrencies in the dark web between January 2017 and March 2018 (Lee et al., 2019). They found that Bitcoin accounted for 99.8% of collected crypto currency addresses and 80% of them are used for illegal purposes. They also estimated the market size is around 180 million USD. Foley et al. (2019) investigated Bitcoin transactions between January 3, 2009 and the end of April 2017 to estimate illegal activity by network cluster analysis and a regression approach called detection-controlled estimation. It showed that Bitcoin worth around 76 billion USD per year was used in dark web market places, and accounted for 46% of all Bitcoin transactions.

3. Methodology

3.1. Bitcoin transaction

Before introducing the measurement methods, we show how Bitcoin transactions are recorded using the AlphaBay addresses.\(^1\) Bitcoin users have wallets that can contain any number of Bitcoin addresses. Each address, adr, is mapped through a transformation function to a unique public/private key pair. A transaction between the addresses of a sender, \(a_s\), and the addresses of a receiver, \(a_r\), has the following form:\(^2\)

\[
\tau = (S, B, a_r; \text{sig}(sk(a_s))) (S, B, a_r) \quad \text{where} \quad \text{sig}(sk(a_s)) \quad \text{is the signature using the private key} \quad sk(a_s) \quad \text{that corresponds to the public key associated with} \quad a_s, \quad B \quad \text{is the amount of Bitcoin (BTC) transferred to} \quad a_r, \quad h \quad \text{is the time (shown as block height) when the validity of the transaction is confirmed in the Bitcoin network, and} \quad S \quad \text{is a reference to the most recent transaction that} \quad a_s \quad \text{acquired the BBTC from. Note that the information of the wallets is not revealed so as to preserve the privacy of the Bitcoin holders and transactions.}
\]

Fig. 1 shows how each Bitcoin transaction is recorded. There are five Bitcoin addresses,\(^3\), on the left-hand side as the input. There are two Bitcoin addresses,\(^4\) \(a_r\), on the right-hand side as the output. It can be seen that there is a transaction from the addresses \(a_s\) of the input on the left-hand side to the addresses \(a_r\) of the output on the right-hand side. The former address of the output received 0.21BTC, and the latter received 0.01BTC. To set the input, users must know the secret private key \(sk(a_s)\) of the addresses, and users who have several addresses control their secret private keys. Thus, addresses recorded as input in one transaction are owned by the same user (Reid and Harrigan, 2013). This is the first heuristic used to identify transactions in the dark web marketplaces,\(^5\) which has been used in previous studies (Androulaki et al., 2013; Meiklejohn et al., 2013; Reid and Harrigan, 2013). The formal description is given as follows:

**Heuristic 1.** If more than two addresses are inputs to the same transaction, they are owned by the same user. Thus, for any transaction \(\tau_h\), all \(adr \in a_s\) are owned by the same user.

3.2. Identifying marketplaces transactions

To purchase illegal goods and services, users transfer their Bitcoins to the site’s Bitcoin addresses. The Bitcoins sent by users are held in escrow until the transactions are completed. After a transaction is completed and the marketplace takes a commission fee, the marketplace sends the Bitcoins to the vendor.

To identify transactions in the dark web marketplaces via Bitcoin transactions, Bitcoin addresses owned by these marketplaces are required. Part of the Bitcoin addresses owned by the dark web marketplaces are publicly available owing to voluntary efforts by the community and measures adopted by legal authorities. Let \(adr市场规模\) denote a set of known addresses owned by each marketplace. Note that the administrators send information of their Bitcoin addresses to users and vendors for escrow. Therefore, their Bitcoin addresses are likely to be revealed in public. These known addresses are the starting point, and the next step is to ascertain whether there are other unknown addresses owned by these marketplaces and find such unknown addresses if necessary.

To this end, internal transactions among known addresses owned by each marketplace are examined. Specifically, given any addresses such that \(adr市场规模\), \(adr市场规模\) such unknown addresses if necessary.

\(\text{Table 2 shows the internal transactions of 1000 randomly selected addresses among the addresses owned by each marketplace. For AlphaBay, it shows that} 0.01BTC transactions account for 98.1% and transactions above 0.1BTC account for 1.2% of all the internal transactions. The rest of the marketplaces also shows a similar distribution of internal transactions among addresses owned by each dark web marketplace. Table 2 indicates that 0.01BTC transactions account for more than 85% of all the internal transactions on all the marketplaces except Evolution. Remarkably, Bitcoin transactions above 0.1BTC account for at most about 10% of all the internal transactions on all the marketplaces but Evolution. Here, the second heuristic used to identify transactions in the dark web marketplaces is formally described as follows:

**Heuristic 2.** If an address is an input (output) to the transaction that the known addresses of a dark web marketplace as an output
AlphaBay’s 0.01BTC transaction as well as the rest of the corresponding transactions of users. For this purpose, the purpose of sending 0.01BTC is to anonymize and secure transactions was common to all the marketplaces although it was not necessary.

In the next step is to ascertain whether there are other unknown addresses owned by such marketplaces and no other major tools has not been introduced to start up dark web marketplaces. It is likely that the observed pattern of internal transactions of 0.01BTC in the seven dark web marketplaces suggests that these dark web marketplaces use the same software to manage Bitcoins. It is likely that the purpose of sending 0.01BTC to anonymize and secure transactions of users. For this purpose, bitwasp has been available from then on. Furthermore, bitwasp is called ‘Silk Road-like’ software and no other major tools has not been introduced to start up dark web marketplaces. It suggests that the six marketplaces launched after Silk Road inherited a legacy of Silk Road although it is difficult to identify that bitwasp was the one that those marketplaces used. AlphaBay’s 0.01BTC transaction as well as the rest of the marketplaces are related. The rationale that the six marketplaces are Silk road-like is that the feature of 0.01BTC internal transactions was common to all the marketplaces although it was not necessary.

The average number of transactions that 0.01BTC was sent (received) by the known addresses owned by Nucleus to (from) the outside addresses is nearly closed in all the marketplaces but AlphaBay. In AlphaBay, the number of transactions is much higher than the rest. Nucleus left its addresses that 0.01BTC transactions were sent to as they were, and thus those addresses were counted as the outside addresses. It results in falsely high average number of transactions that 0.01BTC was sent (received) by the known addresses owned by Nucleus to (from) the outside addresses. Note also that there are no transactions on Silk Road identified before May 2012.

Therefore, such addresses revealed by public efforts are identified as the addresses owned by the six marketplaces. Based on these addresses, transactions with addresses outside the marketplaces that have such addresses as output can be traced and identified as purchases on those marketplaces. A heuristic for identifying purchases on all the marketplaces but AlphaBay is defined as follows:

Heuristic 1. If a transaction of addresses not owned by dark web marketplaces as input has the addresses owned by dark web marketplaces as output, then such a transaction is identified as a purchase on these marketplaces. Thus, if \( \tau_r(\text{adr}_s \rightarrow \text{adr}_r) = (S, B, \text{adr}_r, \text{sig}_{\text{dark}}(S, B, \text{adr}_r)) \) such that \( B' \subset B \) = 0.01 for any \( \text{adr}_r \subset \text{adr}_r \subset \text{adr}_r \subset \text{adr}_r \subset \text{adr}_r \). \( \text{adr}_r \) is owned by a dark web marketplace.

The observed pattern of internal transactions of 0.01BTC in the seven dark web marketplaces suggests that these dark web marketplaces use the same software to manage Bitcoins. It is likely that the purpose of sending 0.01BTC to anonymize and secure transactions of users. For this purpose, bitwasp has been available from then on. Furthermore, bitwasp is called ‘Silk Road-like’ software and no other major tools has not been introduced to start up dark web marketplaces. It suggests that the six marketplaces launched after Silk Road inherited a legacy of Silk Road although it is difficult to identify that bitwasp was the one that those marketplaces used. AlphaBay’s 0.01BTC transaction as well as the rest of the marketplaces are related. The rationale that the six marketplaces are Silk road-like is that the feature of 0.01BTC internal transactions was common to all the marketplaces although it was not necessary.

The average number of transactions that 0.01BTC was sent (received) by the known addresses owned by Nucleus to (from) the outside addresses is nearly closed in all the marketplaces but AlphaBay. In AlphaBay, the number of transactions is much higher than the rest. Nucleus left its addresses that 0.01BTC transactions were sent to as they were, and thus those addresses were counted as the outside addresses. It results in falsely high average number of transactions that 0.01BTC was sent (received) by the known addresses owned by Nucleus to (from) the outside addresses. Note also that there are no transactions on Silk Road identified before May 2012.

Therefore, such addresses revealed by public efforts are identified as the addresses owned by the six marketplaces. Based on these addresses, transactions with addresses outside the marketplaces that have such addresses as output can be traced and identified as purchases on those marketplaces. A heuristic for identifying purchases on all the marketplaces but AlphaBay is defined as follows:

Heuristic 2. If a transaction of addresses not owned by dark web marketplaces as input has the addresses owned by dark web marketplaces as output, then such a transaction is identified as a purchase on these marketplaces. Thus, if \( \tau_r(\text{adr}_s \rightarrow \text{adr}_r) = (S, B, \text{adr}_r, \text{sig}_{\text{dark}}(S, B, \text{adr}_r)) \) such that \( \text{adr}_r \subset \text{adr}_r \subset \text{adr}_r \subset \text{adr}_r \). \( \text{adr}_r \) is identified as a purchase on dark web marketplaces.

Transactions of 0.01BTC outside the addresses owned by all the marketplaces but AlphaBay are not traced because of the risk of false identification. There can be transactions of 0.01BTC that are not related to these dark web marketplaces. Legitimate transactions with 0.01BTC can take place. Transactions on the six marketplaces are identified using Heuristic 3, and Bitcoin prices in terms of USD are used to estimate sales volumes in USD. To calculate the sales volume of each transaction, the end-of-day Bitcoin price on the date of transaction is used. Aggregating all transactions within a given month and multiplying by the end-of-day Bitcoin price gives the daily sales volume in each marketplace. The monthly sales volume is calculated by aggregating the daily sales volume within a given month.

3.2.1. Silk Road, Silk Road 2.0, Agora, Evolution, Nucleus, and Abraxas

The next step is to ascertain whether there are other unknown addresses owned by such marketplaces and find these unknown addresses if necessary. The 0.01BTC transaction among its own addresses is nearly closed in all the markets but AlphaBay. In other words, these addresses owned by the respective marketplaces rarely have transactions of 0.01BTC with non-owned addresses. There are 350,036 known addresses owned by Silk Road. The average number of transactions that 0.01BTC was sent (received) by those known addresses owned by Silk Road to (from) non-owned addresses is 0.037.\(^6\) The corresponding figures are 372,753 and 0.061 for Silk Road 2.0, 498,001 and 0.067 for Agora, 420,615 and 0.002 for Evolution, 146,381 and 0.730 for Nucleus, and 119,065 and 0.125 for Abraxas. Note that the ratio for Nucleus is much higher than the rest. Nucleus left its addresses that 0.01BTC were sent to as they were, and thus those addresses were counted as the outside addresses. It results in falsely high average number of transactions that 0.01BTC was sent (received) by the known addresses owned by Nucleus to (from) the outside addresses. Note also that there are no transactions on Silk Road identified before May 2012.

Therefore, such addresses revealed by public efforts are identified as the addresses owned by the six marketplaces. Based on these addresses, transactions with addresses outside the marketplaces that have such addresses as output can be traced and identified as purchases on those marketplaces. A heuristic for identifying purchases on all the marketplaces but AlphaBay is defined as follows:

Heuristic 3. If a transaction of addresses not owned by dark web marketplaces as input has the addresses owned by dark web marketplaces as output, then such a transaction is identified as a purchase on these marketplaces. Thus, if \( \tau_r(\text{adr}_s \rightarrow \text{adr}_r) = (S, B, \text{adr}_r, \text{sig}_{\text{dark}}(S, B, \text{adr}_r)) \) such that \( \text{adr}_r \subset \text{adr}_r \subset \text{adr}_r \). \( \text{adr}_r \) is identified as a purchase on dark web marketplaces.

Transactions of 0.01BTC outside the addresses owned by all the marketplaces but AlphaBay are not traced because of the risk of false identification. There can be transactions of 0.01BTC that are not related to these dark web marketplaces. Legitimate transactions with 0.01BTC can take place. Transactions on the six marketplaces are identified using Heuristic 3, and Bitcoin prices in terms of USD are used to estimate sales volumes in USD. To calculate the sales volume of each transaction, the end-of-day Bitcoin price on the date of transaction is used. Aggregating all transactions within a given day and multiplying by the end-of-day Bitcoin price gives the daily sales volume in each marketplace. The monthly sales volume is calculated by aggregating the daily sales volume within a given month.

3.2.2. AlphaBay

There are 189,776 known addresses owned by AlphaBay. The average number of transactions that 0.01BTC was sent (received) by those known addresses owned by AlphaBay to (from) non-owned addresses is 0.222. It is unlikely that 0.01BTC transactions among its own addresses are closed in the known addresses because the average number of transactions is four times larger than that on Agora. More importantly, the number of known addresses, i.e., 189,776, is relatively small compared to the number of addresses (more than 340,000) found by legal authorities (United States District Court, 2017). Thus, there are many unknown addresses owned by AlphaBay and it is necessary to trace and identify these unknown addresses using Heuristic 1 and Heuristic 2. To this end, the following algorithm is established.

Algorithm.
Step of the algorithm was iterated five times for each newly obtained AlphaBay address because five iterations resulted in a total of 595,819 addresses, which is larger than the number of addresses (more than 340,000) found by the FBI (United States District Court, 2017). This method may detect many addresses that are not related to AlphaBay; hence, too many iterations result in large number of addresses that are not in fact related to AlphaBay. Note that transactions or revenues after March 2016 cannot be estimated in principle because AlphaBay changed its transaction management around the end of February 2016 according to our investigation of identifying transactions on AlphaBay. The addresses identified as those owned by AlphaBay until February 2016 had less transactions since March 2016. Furthermore, there were almost no 0.01BTC transactions by the known addresses, and thus, Heuristics 2 and 3 had no longer worked. Owing to the system change, transactions on AlphaBay can no longer be traced with the heuristic that we found. However, the FBI mentioned that AlphaBay changed its system in April 2016. Therefore, the period between March and April 2016 can be a transition period, and its transactions are identified during the period. Heuristic 3 is used to identify transactions on AlphaBay. The algorithm identifies transactions on AlphaBay for the first half of its lifetime. It suggests that the dark web marketplaces departed from the legacy of Silk Road.

3.3. Advantages and limitations

The methodology used in this paper has advantages over the established method of web-scraping, given that addresses owned by dark web marketplaces are correctly identified. The newly introduced method based on Bitcoin transactions provides accurate records of sales volumes and dates for each purchase. Thus, it provides comprehensive pictures of sales volumes and revenues for any frequency (e.g., daily, monthly, and overall active period). This is because records of Bitcoin transactions include the amount of Bitcoins used and the exact date.

Scraping methods cover information incompletely; thus, they are likely to provide lower bound estimates. Incomplete data coverage has two forms: incomplete information of prices and quantities, and incomplete coverage of activity. The scraping method collects information on prices and quantities of goods and services from the listings on the marketplaces. The realized prices and quantities can be different from those of the listings. The previous studies assumed that a listing price was a realized price, and a single quantity was purchased for conservative estimation.

Next, the market development over time may be inaccurate because the scraping method cannot cover the entire lifetime of a certain dark web marketplace. To scrape information of dark web marketplaces, one needs information that they exist and are active. However, as they are underground, it is difficult to trace their listings from their birth periods. The Bitcoin method does not suffer from these issues.

The new method proposed here focuses on a feature of Bitcoin transaction management shared by the seven marketplaces, i.e., Heuristics 2 and 3. Research based on Bitcoin transactions uses Heuristic 1 and tracks the Bitcoin balance held by Silk Road.

According to this heuristic, which was newly revealed by the investigation of internal transactions via addresses owned by each marketplace, a more general examination can be conducted. In particular, few studies have focused on Evolution, Nucleus, and Abraxas.

There are certain drawbacks. It is the most crucial that the Bitcoin addresses of dark web marketplaces may not be correctly identified. There are two types of errors: false positive (mis-detection) and false negative. Our method suffers from mis-detection more seriously because there can be Bitcoin transactions of 0.01BTC that are not related to the dark web marketplaces. Another drawback is that it is impossible to determine the price and quantity from the sales volume information. In addition, product categories cannot be determined by the method of Bitcoin transactions.

Therefore, this study complements the scraping methods and provides supporting evidence revealed in the previous studies. However, the misdetection rate should be modest because more than 80% of Bitcoin addresses on the dark web were used with illegal purposes (Lee et al., 2019).

4. Results

4.1. Monthly sales volumes

The total sales volumes of the dark web marketplaces are 192.7 million USD between June 2012 and October 2013 on Silk Road, and 166.0 million USD between December 2014 and February 2016 on AlphaBay. The corresponding figures are 112.9 million USD on Silk Road 2.0, 220.7 million USD on Agora, 69.7 million USD on Evolution, 88.3 million USD on Nucleus, and 35.6 million USD on Abraxas for their entire lifetime. The average monthly sales volumes are 10.7 million USD for Silk Road, 8.7 million USD for Silk Road 2.0, 10.5 million USD for Agora, 4.7 million USD for Evolution, 4.9 million USD for Nucleus, 3.0 million USD for Abraxas, and 1.1 million USD for AlphaBay during the observed period. AlphaBay continued operation until June 2017 and appeared to have made even larger sales after the observed period. Therefore, AlphaBay appeared to be the most successful dark web marketplace until its closure. Our results are generally consistent with the previous studies and also provide new insights. Our estimates including those dark web marketplaces were 161 million USD in 2013, 227 million USD in 2014, and 366 million USD in 2015. These estimates also confirmed that the dark web marketplaces identified in 2014 and 2015 earned Bitcoins worth 254 million USD and 357 million USD, respectively (CHAINALYSIS, 2019).

Fig. 2 shows the monthly sales volume over time for each marketplace. It clearly shows how the revenues for each marketplace developed over time and how and when the leading positions changed between the marketplaces. Silk Road grew steadily, and Silk Road 2.0 grew rapidly and reached its peak at more than 13 million USD in January 2014 after the shut down of Silk Road. Agora started its operation in December 2013, and its monthly sales volume steadily increased to more than 12 million USD in November 2014 until the monthly sales volume of Evolution exceeded that of
A few addresses appeared multiple times in a single market, and a few addresses appeared in one marketplace and then in other marketplaces. Additionally, note that users can use different addresses for trading in the dark web marketplaces for anonymity. The same applies to user migration to the rest of the marketplaces.

10 A few addresses appeared multiple times in a single market, and a few addresses appeared in one marketplace and then in other marketplaces. Additionally, note that users can use different addresses for trading in the dark web marketplaces for anonymity. The same applies to user migration to the rest of the marketplaces.
630,000 transactions on Agora, 260,000 transactions on Evolution, 270,000 transactions on Nucelus, 130,000 transactions on Abraaxas for their lifetimes. In terms of the transaction volumes, AlphaBay was the largest and most successful marketplace when it was active. Fig. 3 shows the monthly transaction volumes for each marketplace. It indicates that the popularity of these marketplaces does not differ between the sales and transaction volumes.

To illustrate the characteristics of purchases on the seven dark web marketplaces, Table 3 shows the distribution of expenditures per purchase on those marketplaces. The majority of purchases on all the marketplaces except Silk Road and Nucelus are less than 100 USD. AlphaBay and Abraaxas had a higher ratio, more than 60%, of purchases worth less than 100 USD while the distributions of expenditures per purchase on Silk Road 2.0, Agora, and Evolution were similar. Purchases worth more than 1000 USD accounted for less than 10% on all the marketplaces. Thus, the large fraction of purchases on the seven dark web marketplaces are worth less than 100 USD, and purchases worth more than 1000 USD account for only a small percentage of all the purchases. Thus, it is conjectured that users of the dark web marketplaces buy illegal products and services for their own use and not for resale or wholesale purposes. Motivated by the first academic study on dark web marketplaces that discussed whether the market structure is business-to-business or business-to-consumer (Barratt, 2012), many of the drug studies show that the majority of purchases are for smaller amounts, and most of the revenue comes from larger quantities (Aldridge and Decary-Hétu, 2016; Barratt et al., 2016). Our estimates are consistent with the previous studies.

Fig. 4 shows the average monthly sales volumes per purchase over time. The range of the average monthly sales volumes per purchase on Silk Road, Silk Road 2.0, and Agora that were the first three launched marketplaces is relatively higher than that on the rest of the four marketplaces. The average monthly sales volumes per purchase has a tendency to decrease on Agora, which is in contrast to the upward tendency on Evolution, Nucelus, Abraaxas, and AlphaBay. On those later launched four marketplaces, the average monthly sales volumes were small, i.e., less than 100 USD; however, they increased to more than 200 USD as those marketplaces grew. The decreasing tendency on Agora suggests that purchases on dark web marketplaces attracted more users and became more common and widespread among individual users. In contrast, the increasing tendency on the marketplaces launched after Agora suggests that the users spent more as those marketplaces gained trust. The reversed tendency of the average monthly sales volumes per purchase is likely to indicate that there has been more competition among those dark web marketplaces. The average monthly sales volumes per purchase on the seven dark web marketplaces are also consistent with the previous studies.

<table>
<thead>
<tr>
<th>Marketplaces</th>
<th>Expenditure per purchase ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0–100</td>
</tr>
<tr>
<td>Silk Road</td>
<td>37.4</td>
</tr>
<tr>
<td>Silk Road 2.0</td>
<td>54.1</td>
</tr>
<tr>
<td>Agora</td>
<td>54.0</td>
</tr>
<tr>
<td>Evolution</td>
<td>55.9</td>
</tr>
<tr>
<td>AlphaBay</td>
<td>65.5</td>
</tr>
<tr>
<td>Abraaxas</td>
<td>64.9</td>
</tr>
<tr>
<td>Nucelus</td>
<td>47.8</td>
</tr>
</tbody>
</table>

Fig. 4. Average monthly sales volumes per purchase between June 2012 and April 2016.

5. Discussion

This section discusses implications of our estimates. The implications for privacy in Bitcoin transactions, dark web marketplaces, and public policy are discussed. First, anonymity in Bitcoin transactions is not very high, as our method identified transactions on the seven dark web marketplaces although individual identities were not revealed. However, further investigation by aggregating these transactions by individuals may reveal a personal identity in society. Through a simulation that mimics the use of Bitcoin within a university, the anonymity of Bitcoin was shown to be overestimated (Androulaki et al., 2013). It was shown that the profiles of around 40% of the users could be recovered even with the adoption of privacy measures recommended by Bitcoin.

Second, the attention paid to privacy-enhancing tools that enable participants to keep their transactions and identities secret differs among administrators. Table 2 illustrates this point by showing the internal transactions of 1000 randomly selected addresses among the addresses owned by each marketplace although the purchases on the seven marketplaces are relatively easily identified by a few simple heuristics as shown. It can be seen that 0.01BTC transactions account for more than 90% of all the internal transactions on all the marketplaces except Evolution. Remarkably, Bitcoin transactions above 0.1BTC account for less than 10% of all the internal transactions on all the marketplaces but Evolution. Those transactions are likely to be those for aggregating revenues from sales. Silk Road 2.0, Nucelus, and AlphaBay seem to carefully divide its internal transactions into a large number of transactions with a small amount, motivated by increasing the difficulty in tracing its transactions. Silk Road, Agora, and Abraaxas seem to be moderately careful; however, Evolution did not appear to pay attention to aggregating revenues. It is suggestive that the marketplaces with the higher internal transactions ratios, Agora, Nucelus, and AlphaBay, increased their sales volumes rapidly.

Recently, vendors have increasingly focused on their privacy. This is supported by observing the effects of Operation Bayonet, an international policing effort undertaken in the summer of 2017 against AlphaBay and Hansa Market (Van Wegberg and Verburgh, 2018), which led to vendors’ migration to a dark web marketplace named Dream Market. The migration pattern of the vendors differed between AlphaBay and Hansa Market. The vendors on AlphaBay migrated with their previous user names and thus reputation, whereas a few of the Hansa Market vendors did so and

---

11 As indicated in footnote 10, it is not feasible to measure the purchase frequencies of users.


Therefore, our identification algorithm and the resulting estimation are not affected by the use of cryptocurrencies other than Bitcoin.