Monitoring Product Sales in Darknet Shops

York Yannikos
Fraunhofer Institute for Secure Information Technology SIT
Darmstadt, Germany
york.yannikos@sit.fraunhofer.de

Annika Schäfer
Technische Universität Darmstadt
Darmstadt, Germany
annika.schaefer@stud.tu-darmstadt.de

Martin Steinebach
Fraunhofer Institute for Secure Information Technology SIT
Darmstadt, Germany
martin.steinebach@sit.fraunhofer.de

ABSTRACT

Anonymity networks and hidden services like those accessible in Tor, also called the "darknet", in combination with cryptocurrencies like bitcoin provide a relatively safe environment for criminal online activities. While this is a challenge for law enforcement, it brings opportunities for researchers to monitor these activities as they are often not really hidden but rather obfuscated and/or anonymized. In this paper we discuss such a monitoring approach for product sales in the darknet. We collect bitcoin addresses and data about product offerings in a number of shops run as hidden services in Tor. We then analyze transactions in the bitcoin blockchain that can be mapped to specific product sales in these shops.

KEYWORDS

Darknet product sales; bitcoin monitoring; web scraping

ACM Reference Format:
York Yannikos, Annika Schäfer, and Martin Steinebach. 2018. Monitoring Product Sales in Darknet Shops. In *Proceedings of International Conference on Availability, Reliability and Security (ARES 2018).* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3230833.3233258

1 INTRODUCTION

The Tor network is often used as a synonym for the hidden parts of the Internet called the "darknet". An important functionality of Tor is the possibility to host hidden services. These services, e. g., web servers, can be operated anonymously without disclosing sensitive information about location or owner. Besides beneficial applications of hidden services, e. g., censorship circumvention in oppressive countries, one application is to implement marketplaces where customers could buy a wide range of illegal goods while being protected with a cryptographically sound anonymity layer. A central aspect of anonymous product sales in Tor marketplaces is the use of cryptocurrencies like bitcoin. Although every single bitcoin transaction can be traced within the blockchain, the public distributed ledger technology that builds the foundation of bitcoin, the participants are usually completely anonymous.

ARES 2018, August 27–30, 2018, Hamburg, Germany

ACM ISBN 978-1-4503-6448-5/18/08…$15.00
https://doi.org/10.1145/3230833.3233258

Tor marketplaces are highly interesting for research – there have been several studies that looked into type and amount of products offered and sold in Tor marketplaces [2, 10, 12]. These studies used product listings and vendor feedback to determine supply and demand. However, there has not been much work regarding the analysis of sales of specific vendors based on bitcoin transactions connected to these vendors.

Contributions

In this paper we describe a concept to monitor product sales in Tor marketplaces and shops: we utilize bitcoin transactions gathered from the blockchain to derive information about connected product sales. In order to identify relevant bitcoin addresses of several vendors we use social engineering as well as public information. For the collection of data about vendor product supply we use common web scraping technology.

Outline

This paper is structured as follows: Section 2 provides a brief overview on how bitcoin works in general. In Section 3 we summarize the main aspects of the technology behind Tor and especially hidden services. In Section 4 we propose our concept for monitoring product sales in darknet shops. The results of our concept evaluation are given in Section 5. We discuss related work in Section 6 and give a conclusion in Section 7.

2 BITCOIN TRANSACTIONS

Bitcoin, introduced in 2008 by one or more individuals using the pseudonym "Satoshi Nakamoto" [13], is the first decentralized and currently the most popular cryptocurrency. Unlike a traditional currency, bitcoin does not require a trusted third party like a bank to ensure the validity of a transaction. Instead, this is done by using the blockchain, a public ledger that records bitcoin transactions as a chain of blocks: each block contains a cryptographic hash of the previous block and therefore all bitcoin transactions ever made are public and traceable.

The basis of sending and receiving bitcoins is asymmetric cryptography: Every individual who wants to use bitcoin must create at least one key pair, i. e., one private key and its corresponding public key. The private key is stored in the *bitcoin wallet* and is used to sign outgoing bitcoin transactions, i. e., payments. The public key is used to derive the *bitcoin address* that is used for bitcoin transactions. Since one bitcoin wallet can hold many different private keys, the wallet owner can use many different bitcoin addresses, all belonging to the same wallet, to increase anonymity.

Although the bitcoin addresses of the sender and the receiver in a transaction are publicly known, the identities of the individuals

behind these addresses, the bitcoin wallet owners, are not. Thus the bitcoin cryptocurrency provides reasonable anonymity for illegal businesses as long as a wallet owner carefully avoids linking own bitcoin addresses to personally identifiable information. For every bitcoin transaction, the transaction partners, time, and value is public in bitcoin's blockchain.

3 TOR MARKETPLACES AND SHOPS

The Onion Router or "Tor" is a free overlay network that allows participants to communicate anonymously with each other [11]. Tor is built on a technology called *onion routing* where all traffic is sent through the network on a predefined path of several nodes. For each node a separate asymmetric encryption layer is added that can only be decrypted by that node. Thus each data packet is wrapped in several encryption layers, much like an onion.

Tor also offers the possibility to host *hidden services*. These are typically websites that can only visited within the Tor network. While normal websites outside of Tor can be contacted very easily by resolving the hostname of the website to its corresponding IP address, this does not work for hidden services in Tor. Hidden services use a special *.onion* top-level domain and a hostname that cannot be resolved via DNS but instead is built from the public key of the host. Therefore, contacting such an onion domain does only work in Tor or via Tor proxies.

Hidden services provide an effective way of anonymously hosting content without disclosing the physical location of the host. This makes them attractive for many shady activities such as buying and selling illegal goods. Besides very large Tor marketplaces like "Dream Market" or "Wall Street Market", where many different suppliers offer their goods in a fashion like on Amazon or eBay, there also exist many small shops that offer a far smaller number of products in total. These shops are often specialized in very specific product categories, e. g., counterfeit euro banknotes, handguns, or cannabis.

4 MONITORING PRODUCT SALES

In order to monitor product sales in Tor marketplaces we propose the following approach that is divided into four phases:

(1) Find vendors that offer illegal goods (products) in marketplaces or shop websites.
(2) Collect bitcoin addresses from those vendors that openly list or communicate their bitcoin address to receive payments.
(3) Collect data from vendor pages in marketplaces or shop websites using web scrapers.
(4) Perform an analysis to link products and product prices with payments to vendor bitcoin addresses.

Phase 1: Preparation

In order to find relevant vendors for our monitoring approach, we search aggregation pages like "The Hidden Wiki" or "DeepDotWeb" [3, 9]: these sites provide comprehensive lists of Tor marketplaces where many different products are traded. Smaller shops are more difficult to find as they are a lot less popular, but this can be achieved by manually checking onion addresses from public lists of hidden services.

Phase 2: Collection of Bitcoin Addresses

Although there are plenty of vendors selling their products in Tor, we want to focus on those that disclose at least one of their bitcoin addresses they use for accepting payments. This is especially difficult for large marketplaces like Dream Market as they typically provide an escrow service. Since all payments are done via the escrow service, the transaction partners are generally not required to exchange bitcoin addresses for direct payments. Hence vendors in large marketplaces typically do not list any bitcoin addresses on their vendor page. Therefore, we propose social engineering to collect a sufficient number of bitcoin addresses. In our evaluation, we approached several vendors with a message asking for their bitcoin address in order to initiate a deal off-site.

For smaller shops it is far more common to openly list a bitcoin address for payments, i. e., on the shop website. In order to add more anonymity to their bitcoin transactions, some shops use dynamically generated bitcoin addresses that are different for each visitor and therefore do not have a bitcoin transaction history. However, many shops list only one single bitcoin address that can be easily collected automatically.

Phase 3: Scraping of Product Lists

To monitor the list of products offered by the vendors in our scope, one web scraper has to be implemented for each vendor shop or vendor page on a marketplace. The minimum amount of information a scraper must be able to reliably collect are product titles and prices. The scraper must also provide robust error handling, e. g., for cases when web requests or required login sessions time out.

Compared to web scrapers for normal websites outside Tor, the only additional technical requirement for a web scraper to collect data from Tor hidden services is support for SOCKS proxy connections. This means that many common web scraping libraries can be also be used for scraping in Tor, because the default Tor client comes with a SOCKS proxy. Other difficulties like login pages, request throttling, CAPTCHAs, or timeouts have to be handled in the same way like on normal websites outside Tor.

After a scraper for each vendor page/shop has been implemented and set up, monitoring can be started. The main purpose of a continuous monitoring is the detection of any price change in the product range of the vendor. To get an idea about how often scraping per vendor page is required, i. e., how often price changes are likely to occur, we think it is useful to do a test run over a few days. After the test run is finished, we can derive a suitable scraping frequency per vendor page.

Phase 4: Linking Bitcoin Transactions to Product Sales

While scraping the vendor pages is time-critical, i. e., it is required to memorize the exact time frame in which the data was scraped, the analysis of the bitcoin transactions of the corresponding vendors is not: All transactions are stored in the blockchain and can be used for analysis even much later. Therefore, we suggest to first completely finish the scraping process for all vendor pages before conducting the bitcoin transaction analysis.

For the analysis of the bitcoin transactions, i. e., finding those transactions that are most likely linked with a product sale, we suggest the following steps:

(1) Fetch the list of all bitcoin transactions for a vendor from the blockchain.
(2) Convert the transaction values from bitcoin to US dollar or euro using the exchange rate at that time.
(3) Compare the converted transaction values with the product prices of the vendor at that time.

Both the bitcoin transactions as well as historical exchange rates can be gathered from various bitcoin exchange websites, ideally those that provide access to an API. After converting the bitcoin transaction values to US dollar or euro, they can be compared to the data collected in the scraping phase. If values match a specific product price and are non-ambiguous, we consider the corresponding bitcoin transaction as a payment for a sale of this product. We suggest to use some degree of tolerance when comparing the values with the collected product prices and also consider shipping costs if mentioned on the vendor page.

5 EVALUATION

In this section we describe how we applied each phase of our monitoring approach.

Preparation and Implementation

For our analysis we first chose 5 marketplaces based on popularity and uptime (as reported on DeepDotWeb) as well as accessibility (we only chose marketplaces with an open registration process and disregarded any invite-only marketplaces) and complexity of their website structure. This resulted in the following marketplaces: AlphaBay, Dream Market, Outlaw Market, Tochka, and Zion.

On these 5 marketplaces we started our search for vendor bitcoin addresses with social engineering. We sent 65 vendors a message asking for their bitcoin address by proposing an off-site deal. The results are summarized in Table 1. Unfortunately, we only got 34 replies with mainly refusals. 14 vendors accepted our proposal and sent a bitcoin address or other contact information. We were able to collect nine bitcoin addresses, three email addresses, two phone numbers, and one skype contact. Of the bitcoin addresses only four had been used earlier for transactions, the other five bitcoin addresses had not been used. One of the four addresses with a transaction history belonged to a vendor on AlphaBay – this marketplace was taken offline before we had finished implementing our scraper [4]. The owner of one of the remaining three bitcoin addresses got his account banned on the marketplace. In the end we were able to collect only two bitcoin addresses using social engineering.

After the lack of success with our social engineering approach, we searched several websites providing lists of Tor hidden services (i. e., onion addresses) and manually checked the lists for single vendor shops. In total we found 188 single vendor shops. Of these, 138 were not usable for our research mostly because the listed bitcoin address had no transaction history or the bitcoin address was not shown at all. Some shops did not list any product prices to collect and compare bitcoin transactions with. Of the remaining 50 shops with accessible bitcoin addresses with a transaction history, 12 listed addresses that contained either very old transactions or only a single one. 17 shops listed bitcoin addresses belonging to the same wallet as other shops that offered completely different products. Thus we assumed that these shops were using additional anonymizing services for bitcoin transactions. Of the remaining 21 shops 3 went offline before we could finish implementing a scraper.

Table 1: Information collected after contacting 65 vendors

Information	Amount
No reply	31 (48%)
Replies with refusals	20 (30%)
Replies with further information	14 (22%)
Bitcoin addresses with transaction history	4
Bitcoin addresses without transaction history	5
Email addresses	3
Phone numbers	2
Skype contacts	1

In total we were able to collect bitcoin addresses from two vendors selling their products on large marketplaces and from 18 single vendor shops. This resulted in 20 bitcoin addresses that we could use for monitoring.

Data collection

To continuously monitor the bitcoin transactions of each vendor we implemented a client for the BlockTrail API [8]. This provided us with access to all bitcoin transaction data without having to download and work with the whole blockchain. Although the BlockTrail API did have a request limit (300 requests per minute), we did not reach this limit.

For each of the 20 vendor pages we implemented a scraper that was able to collect the list of products offered (title and price) as well as additional information about shipping costs, if available. We noticed that some vendors regularly changed the bitcoin address listed on their page – for those we implemented an additional routine in the scraper to update their bitcoin address in our database to the one currently listed. The implementations for communicating with the BlockTrail API as well as for web scraping were done in Python.

After all implementations were finished, we did a scraping test run for one week to get an idea about how often product lists, prices, and the bitcoin address of the corresponding vendor changed and how often errors occurred that needed special handling. During the test run all scrapers ran three times a day. After the test run we found that we only needed to scrape all vendor pages once a day because neither the product lists nor the prices changed more frequently. We then started the scraping phase where our scrapers ran for a total duration of 14 weeks from September to December 2017. The following analysis is the based on the data collected during this scraping phase.

Analysis

During the scraping phase we observed a total of 1754 bitcoin transactions. One interesting finding was that three of the 20 shops did

not receive any transaction at all while two other shops received more than 500 transactions each. Of the 1754 transactions we had to dismiss 379 (22%) due to the following reasons: either our scrapers were not able to fetch data in the corresponding time frame, i. e., the vendor page was not reachable during that time, or the transaction value was far below the lowest price for a product of the corresponding vendor. We assume that the transactions in the latter case were change from another transaction. For the remaining 1375 bitcoin transactions we analyzed which products were most likely the ones paid for. We identified 107 transactions (8%) with a value that exceeded the highest product price of the corresponding vendor by a very high amount (up to 20 times). We concluded that these transactions were payments for bulk orders. Because we also saw that the corresponding vendors had wide product ranges with many different products, we did not further analyze all possible combinations that could have resulted in these transaction values. Table 2 shows the number of transactions we could observe during the scraping phase.

Table 2: Number of transactions during the scraping phase

Total	1754
Dismissed	379
Analyzed	1375
More than one product (bulk orders)	107
No match / partly ambiguous	244
Ambiguous	649
Distinct	375

244 of the 1375 transactions (18%) had a value that did not exceed the highest product price of the corresponding vendor but could not be matched to a single product. Further analysis showed that many of these transaction values were most likely the sum of several low-price products of the vendor. For each of the remaining 1024 transactions we were able to identify at least one product of the corresponding vendor with a price that matched the transaction value (5% tolerance, including shipping costs if data was available). We categorized these transactions as follows:

- *Ambiguous transaction:* transaction value matched price of several single products or the sum of a group of products.
- *Distinct transaction:* transaction value matched price of a single product.

Table 3 shows the number of transactions per vendor during the scraping phase, Table 4 and Figure 1 show the total, average, and median transaction values as well as the number of analyzed transactions per vendor. The columns of the tables describe the following:

Vendor	Name of the vendor
Category	Name of the main product category of the vendor
T_{total}	Total number of incoming transactions of the vendor's bitcoin address during the scraping phase
T_{analyzed}	Number of transactions that could be further analyzed (i. e., total minus dismissed transactions)
P_{distinct}	Number of distinct products of the vendor (i. e., not counting same product in different quantity)
Bulk orders	Number of transactions that were most probably payments for bulk orders due to a very high transaction value
No match	Number of transactions that did not exceed the highest product price of the vendor but could not be matched to a single product
$T_{\text{ambiguous}}$	Number of ambiguous transactions – in brackets: share of transactions with no match (previous column)
T_{distinct}	Number of distinct transactions
Total	Total value of all transactions in bitcoin
Average	Average value of all transactions in bitcoin
Median	Median value of all transactions in bitcoin

Several vendors offered their products in different quantities often granting volume discounts. In these cases we considered it to be very likely that the buyer would take the discount offer to get a larger amount of the product for the same price. Some vendors shown in Table 3 did not receive any transactions or were offline or could not by scraped for some time when they received a transaction ($T_{\text{total}} = 0$). Other vendors shared the same bitcoin address and showed a high similarity in offered products. We considered these vendors to be the same entity hosting multiple shops, e. g., "LimaConnection" and "RosarioCocaine".

The two vendors "CharlieUK" and "TheToYouTeam" had significantly more incoming transactions than all other shops while offering a very small range of distinct products. The vendor "GC4You" offered only one distinct product (gift cards) but with different values. We divided the products offered by the vendors into five categories:

- Counterfeit money
- Drugs
- Financial
- Gift cards
- Gold & Jewelry

Vendors in the "Financial" category offered either fraud or stolen credit cards, PayPal accounts, or money transfers where the buyer gains more money than spent. Vendors in the "Gift cards" category mainly offered Amazon gift cards where the buyer pays only a fraction of the gift card value.

Table 4 shows that the vendors with most transactions also had the highest total transaction value ("CharlieUK", "TheToYouTeam"). However, some vendors with only a few transactions still received a substantial value, e. g., "RoyalCards" or "LimaConnection / RosarioCocain". As indicated by the significant difference between average and median transaction value, these vendors had incoming transactions with greatly varying value.

Figure 2 shows the aggregated data per product category. We could link 73% of the observed transactions to drug sales, 16% to

Table 3: Number of transactions per vendor during the scraping phase

Vendor	T_{total}	T_{analyzed}	P_{distinct}	Bulk orders	No match	$T_{\text{ambiguous}}$	T_{distinct}
BuyCC	32	31	9	0	3	27 (1)	2
CC-Goldshop	4	4	20	0	0	4 (0)	0
CharlieUK	582	486	2	63	123	296 (99)	103
CreditLW	32	12	5	0	6	6 (0)	0
Dashtor	164	82	25	0	1	56 (0)	25
DreamWeaverz	0	0	2	–	–	–	–
DrugsDark / WebShop	29	27	93	0	1	26 (1)	1
EUCardShop	3	2	14	0	2	0 (0)	0
GC4You	98	80	1	3	12	6 (1)	60
Gold & Diamonds	2	1	7	0	1	1 (1)	0
Here You Get / PP Accounts	0	0	14	–	–	–	–
Jungle	25	15	9	8	4	0 (0)	3
LimaConnection / RosarioCocaine	11	11	2	0	9	5 (3)	0
RoyalCards	21	20	3	4	12	16 (12)	0
ThePPCent	65	63	57	4	11	48 (10)	10
TheToYouTeam	618	481	4	0	55	311 (54)	169
USD4You	35	30	4	25	3	3 (3)	2
WaltCards	31	30	20	0	1	29 (0)	0
german-weed (Tochka)	0	0	10	–	–	–	–
ultimatum2016 (Dream Market)	2	0	56	0	0	0 (0)	0

Table 4: Category and transaction values per vendor in bitcoin (BTC) during the scraping phase

Vendor	Category	T_{analyzed}	Total	Average	Median
BuyCC	Financial	31	1.02160246	0.03295492	0.03190000
CC-Goldshop	Financial	4	0.14703388	0.03675847	0.02582316
CharlieUK	Drugs	486	10.63720495	0.02188725	0.01566500
CreditLW	Financial	12	0.48271513	0.04022626	0.03396220
Dashtor	Financial	82	5.51907023	0.06730573	0.06778510
DrugsDark / WebShop	Drugs	27	0.74432605	0.02756763	0.02446334
EUCardShop	Financial	2	0.00820000	0.00410000	0.00410000
GC4You	Gift cards	80	0.56836902	0.00710461	0.00440031
Gold & Diamonds	Gold & Jewelry	1	0.03980248	0.03980248	0.03980248
Jungle	Gift cards	15	0.48089468	0.03205965	0.02506000
LimaConnection / RosarioCocaine	Drugs	11	1.93399817	0.17581802	0.02958228
RoyalCards	Financial	20	4.39547030	0.21977352	0.05905000
ThePPCent	Financial	63	1.41642955	0.02248301	0.02000000
TheToYouTeam	Drugs	481	12.80055922	0.02661239	0.01790000
USD4You	Counterfeit money	30	0.86525684	0.02884189	0.02196980
WaltCards	Gift cards	30	0.40470000	0.01349000	0.01250000

financial services, and 9% to gift card sales. In contrast to that, 43% of the vendors where we could observe incoming bitcoin transactions fell into the "Financial" category and only 25% into the "Drugs" category.

Figure 3 shows the percentages of analyzed transactions that were distinct, ambiguous, or bulk orders. The three transaction types are not equally distributed within the product categories: for instance, bulk orders were by far most common for counterfeit money. This seems reasonable considering that customers are probably not interested in buying single banknotes of counterfeit money. The high percentage of ambiguous transactions in the categories "Drugs" and "Financial" is due to the fact that most of the vendors

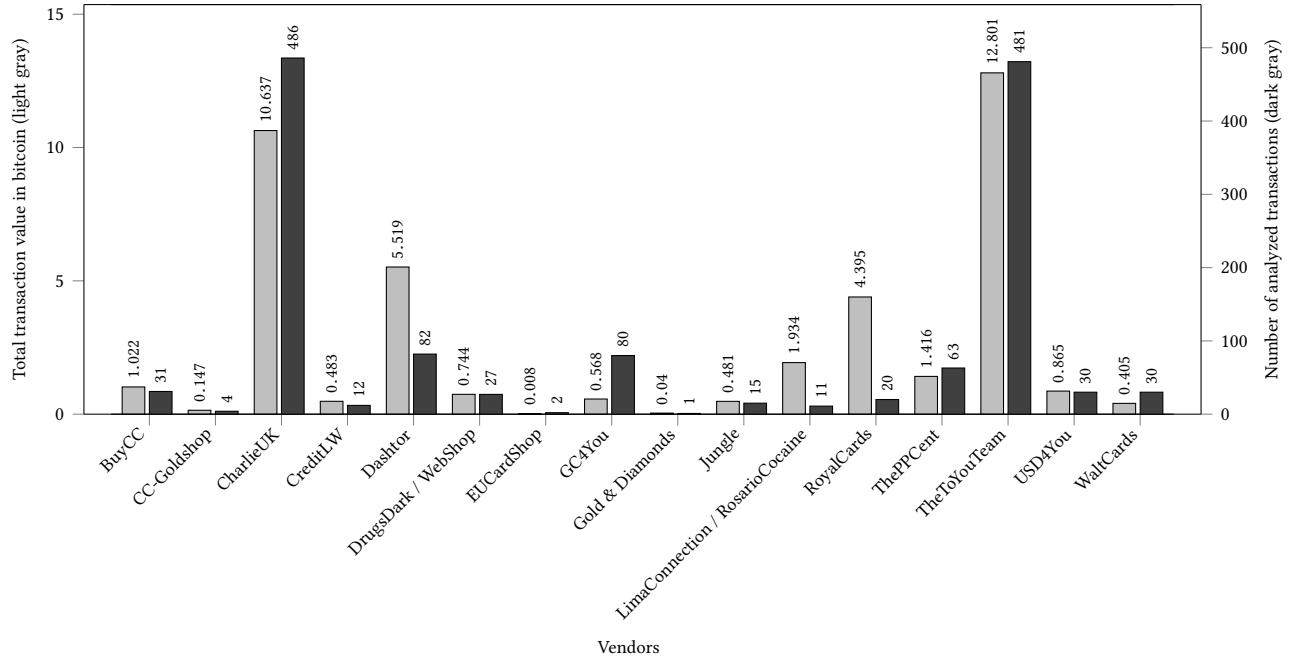

Figure 1: Total value and number of analyzed transactions per vendor

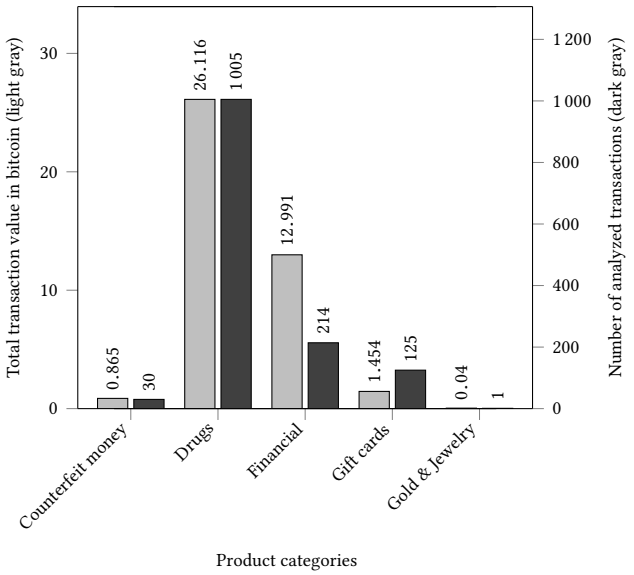

Figure 2: Total value and number of analyzed transactions per product category

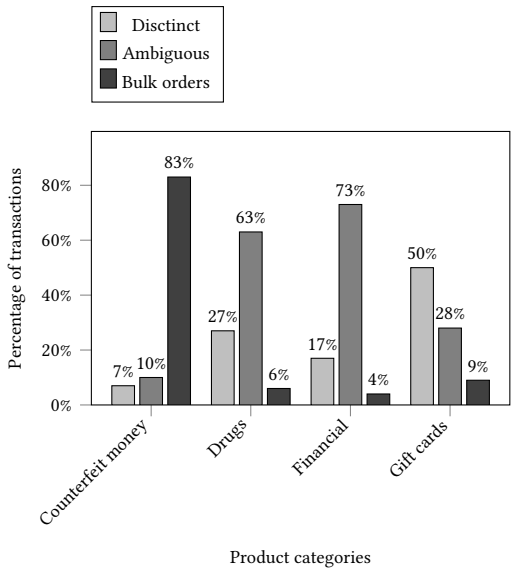

Figure 3: Types of analyzed transactions per product category

in this categories offered a large number of distinct products or many different quantities of their products.

6 RELATED WORK

The anonymous and open nature of darknet markets led to various studies on the topic of darknet drug sales. Rhumorbarbe et al. compared metadata about drug quality in shops with analytic results of purchased samples [16]. In a follow-up activity, the authors used the collected darknet data to derive the relation between real and virtual markets [6]. Broséus et al. scraped information from darknet markets to get a picture about global trafficking [7]. The authors used geographic information on a market about shipping and destination country to analyze the routes the illegal goods take.

Aldridge and Askew discussed obfuscation and detection strategies and compared the possibilities of darknet markets for both police and criminals [1]. Wang et al. scraped darknet markets for product images to detect multiple vendor identities by their usage of identical images [18].

Several works have been published that provide an analysis of bitcoin transactions. Ron and Shamir published a quantitative analysis of the full bitcoin transaction graph [17]. The authors did a thorough analysis on the then existing 3,730,218 bitcoin addresses and provided statistics about the distribution of the number of addresses and the accumulated incoming bitcoins per entity. They were able to associate the total number of addresses to 2,460,814 different entities. Another interesting result was that all very large transactions in the bitcoin blockchain at that time, i. e., with a value of more than 50,000 bitcoins, were descendants of a single transaction from November 2010. Reid and Harrigan derived two networks from the bitcoin transaction history and performed an analysis to deduce informations about bitcoin users [15]. Using external information, the authors then investigated a bitcoin theft with an approximated market value of $500,000 at that time. Ober et al. considered activity of entities in the bitcoin transaction graph and discussed implications on bitcoin anonymity [14]. Biryukov et al. presented a deanonymization attack on bitcoin that allows linking IP addresses to active bitcoin users [5]. The authors also showed that their attack can defeat countermeasures like Tor and proposed mitigation techniques.

7 CONCLUSION

In this paper we proposed an approach to monitor product sales in shops and marketplaces in the Tor network. We evaluated our approach with a data collection running over 14 weeks where we continuously scraped the shops of 20 vendors and performed an analysis using bitcoin transaction data.

While the sample of bitcoin transactions that we could link to product sales may not be very large, the results still show an interesting and important aspect about the nature of such shops and marketplaces. As anonymity is promised, transactions are done openly without much obfuscation beyond the identities of vendors and customers. This allows a much better estimation about criminal activities and revenues coming from it – information otherwise not obtainable without direct access to criminal networks.

Collecting such information would be of value for different parties: scientific disciplines could use it as a basis for further research, for example by comparing normal income with income from drug sales in a country. It could also support future discussions about the pros and cons of Tor and similar anonymity networks by moving away from abstract assumptions towards reliable data samples.

ACKNOWLEDGMENTS

This work is part of the PANDA project (https://panda-projekt.de) and supported by the German Federal Ministry of Education and Research (BMBF).

REFERENCES

[1] Judith Aldridge and Rebecca Askew. 2017. Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy* 41 (2017), 101–109.
[2] Judith Aldridge and David Décary-Hétu. 2014. Not an 'Ebay for Drugs': the Cryptomarket 'Silk Road' as a paradigm shifting criminal innovation. (2014).
[3] Anonymous. 2018. The Hidden Wiki. http://zqktlwi4fecvo6ri.onion
[4] Chris Baraniuk (BBC). 2017. AlphaBay and Hansa dark web markets shut down. http://www.bbc.com/news/technology-40670010
[5] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. 2014. Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 15–29.
[6] Julian Broséus, Marie Morelato, Mark Tahtouh, and Claude Roux. 2017. Forensic drug intelligence and the rise of cryptomarkets. Part I: Studying the Australian virtual market. *Forensic science international* 279 (2017), 288–301.
[7] Julian Broséus, Damien Rhumorbarbe, Marie Morelato, Ludovic Staehli, and Quentin Rossy. 2017. A geographical analysis of trafficking on a popular darknet market. *Forensic science international* 277 (2017), 88–102.
[8] BTC.COM. 2017. BlockTrail API (now BTC.COM API). https://btc.com/api-doc
[9] DeepDotWeb.com Team. 2018. DeepDotWeb. https://www.deepdotweb.com/
[10] Jakob Demant, Rasmus Munksgaard, and Esben Houborg. 2018. Personal use, social supply or redistribution? Cryptomarket demand on Silk Road 2 and Agora. *Trends in Organized Crime* 21, 1 (2018), 42–61.
[11] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. *Tor: The second-generation onion router*. Technical Report. Naval Research Lab Washington DC.
[12] Kristy Kruithof, Judith Aldridge, David Décary-Hétu, Megan Sim, Elma Dujso, and Stijn Hoorens. 2016. Internet-facilitated drugs trade. *Santa Monica, CA/Cambridge, UK: RAND Corporation* (2016), 21–32.
[13] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).
[14] Micha Ober, Stefan Katzenbeisser, and Kay Hamacher. 2013. Structure and anonymity of the bitcoin transaction graph. *Future internet* 5, 2 (2013), 237–250.
[15] Fergal Reid and Martin Harrigan. 2013. An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks*. Springer, 197–223.
[16] Damien Rhumorbarbe, Ludovic Staehli, Julian Broséus, Quentin Rossy, and Pierre Esseiva. 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 science international* 267 (2016), 173–182.
[17] Dorit Ron and Adi Shamir. 2013. Quantitative analysis of the full bitcoin transaction graph. In *International Conference on Financial Cryptography and Data Security*. Springer, 6–24.
[18] Xiangwen Wang, Peng Peng, Chun Wang, and Gang Wang. 2018. You Are Your Photographs: Detecting Multiple Identities of Vendors in the Darknet Marketplaces. (2018).