Are Cryptocurrencies Criminals Best Friends? Examining the Co-Evolution of Bitcoin and Darknet Markets

Full Paper

Christian Janze
Goethe University Frankfurt
janze@wiwi.uni-frankfurt.de

Abstract

While public and private entities question the utility of privacy preserving means of electronic payments for individuals other than criminals, discussions are primarily based on anecdotal evidence. Thus, we address the overall research question of whether pseudonymous cryptocurrencies are primarily used by criminals. Based on Rational Choice Theory and darknet market design, we build a dynamic research model. Utilizing panel data of 296,875 unique product and service listings that were available on 19 darknet markets from June 2014 to July 2015 as well as Bitcoin blockchain transactions, we provide evidence for the co-evolution of Bitcoin and darknet markets. We find that transactions within the Bitcoin blockchain and the usage of transaction obfuscation services can be related to previous sales on darknet markets. The temporal lag can be attributed to escrow mechanisms. We contribute to the research stream of cryptocurrency usage behavior and discussions of regulators, governments and financial services firms.

Keywords

Cryptocurrencies, Bitcoin, Darknet Markets, Co-Evolution, Crime, Rational Choice Theory, Autoregressive Distributed Lag Model.

Introduction

Cryptocurrencies such as Bitcoin allow for pseudonymous peer-to-peer transactions of digital coins via decentralized payment networks (Nakamoto 2008). Their pseudonymous and decentralized nature removes cryptocurrency transactions from the supervision by centralized intermediaries such as commercial and central banks. Thus, they are essentially the digital equivalent of cash.

Critics argue that privacy protecting means of electronic payments are solely useful when considering unlawful activities (Honig 2013; Manchin III 2014) and are thus a dangerous (Fagan 2013) tool benefiting criminals (Mihm 2013). This point of view is shared by the European law enforcement agency Europol, which states that "Bitcoin is establishing itself as a single common currency for cybercriminals within the EU" (EUROPOL 2015). However, despite these claims, little factual knowledge exists regarding the question to what extent cryptocurrency payments originate from illicit activities. Thus, we formulate the overall research question of our study as follows: *Are cryptocurrencies primarily used as a means of payment in criminal activities?*

We operationalize this question by examining the impact of sales on darknet markets on different types of transactions within the Bitcoin blockchain. Darknet markets are hidden services within the Tor network, which allow for buying and selling goods and services such as drugs and fire arms. Based on rational choice theory and the typical design of darknet markets, we derive two research hypotheses and test them empirically. Specifically, relying on a comprehensive data sample of 19 leading darknet markets observed from June 2014 to July 2015, we construct numerous dynamic regression setups based on the Autoregressive Distributed Lag (ADL) framework.

Our results indicate a co-evolution of Bitcoin and darknet markets. First, we show that an increased number of goods and services sold on darknet markets is associated with a time-delayed increased number of transactions within the Bitcoin blockchain. Second, we find indications that an increased

number of goods and services sold on darknet markets are associated with a time-delayed increased usage of Bitcoin transaction obfuscation services approximated by long-chain transactions. We explain these timing dynamics by escrow mechanisms employed by darknet markets. We therefore contribute to the research stream on cryptocurrency usage behavior and ongoing discussions of practitioners and policymakers on the nature of cryptocurrencies.

The remaining portion of this study is structured as follows. Section two provides background information on pseudonymous cryptocurrencies and anonymous darknet markets and presents our research model. Section three presents our data set. Section four outlines our research model. Section five presents and discusses the results of our empirical study. Section six concludes the study and provides directions for future research.

Background and Research Model

Pseudonymous Cryptocurrencies and Criminal Usage Behavior

Cryptocurrencies such as Bitcoin are both a means of payment and payment infrastructure based on peer-to-peer mechanisms (Nakamoto 2008). Their pseudonymous nature makes them a viable alternative for cash to conduct illicit and unlawful activities. While researchers found that it is possible to reveal the identity of Bitcoin users (Androulaki et al. 2013), various coin-mixing services such CoinShuffle (Ruffing et al. 2014) allow for the effective obfuscation of transactions (Moser et al. 2013). Coin-mixing (aka tumbling, laundering) "is the process of using a third party service to break the connection between a Bitcoin address sending coins and the address(s) they are sent to" (Darknetmarkets.org 2015). Thus, coin-mixing services help to mitigate the potential for tracing Bitcoin transactions due to their pseudonymous rather than anonymous nature. Governments and policy makers are increasingly engaged in regulating cryptocurrencies: data compiled by the platform BitLegal.io suggests that as of April 2015, out of 72 jurisdictions, supra-national and intergovernmental organizations investigated, 83.3% exhibit a permissive, 12.5% a contentious and 4.2% a hostile attitude towards cryptocurrencies (Bitlegal.io 2016). With the exception of Sweden, the underlying data is in line with data compiled by CCN.LA (2015), stating that Bitcoin is banned or its usage is discouraged in Bangladesh, Bolivia, China, Ecuador, Iceland, India, Russia, Sweden, Thailand and Vietnam.

Empirical research regarding the usage of cryptocurrencies is sparse: it was shown that Bitcoin is used as an alternative investment vehicle, i.e. a speculative asset rather than a currency (Glaser et al. 2014). Regarding the level of criminal activities, it has been tested whether Bitcoin exchange rates differences across exchanges can be explained by criminal activities (Pieters and Vivanco 2015). Furthermore, Google Trends data has been used to show that Bitcoin interest is primarily driven by computer programming enthusiasts and illegal activities (Yelowitz and Wilson 2015). Furthermore, while scholars argue that “Bitcoin has become both a highly useful tool for criminals and a lucrative target for crime” (Ali et al. 2015), they do not provide empirical evidence for such claims. We therefore argue that the question whether cryptocurrencies such as Bitcoin are primarily used to conduct criminal activities is worthwhile and from an empirical perspective largely neglected.

Anonymous Darknet Markets

Darknet markets were pioneered in February 2011 by the now defunct platform Silk Road that offered its users the possibility to anonymously buy and sell any illicit goods and services but mostly narcotics (Christin 2013). These markets operate similarly to the Amazon marketplace (Soska and Christin 2015). However, in comparison to so-called clearnet markets, darknet markets utilize anonymization technologies such as Tor and I2P to hide both the identities of the darknet market operator as well as its customers. The vast majority of darknet markets are operated as Tor hidden services (see for example Gwen 2015). Tor itself is "a circuit-based low-latency anonymous communication service" (Dingledine et al. 2004). Darknet markets "are hosted on regular servers, but to access them you need special software" (Thompson 2013) such as the Tor browser bundle.

Silk Road was taken down by the U.S. Federal Bureau of Investigation (FBI) in October 2011 and its operator Ross William Ulbricht (aka Dread Pirate Roberts) subsequently sentenced to life in prison (U.S. Attorney’s Office 2015). Shortly thereafter numerous copy cats such as Silk Road 2.0 emerged. However,

on 2014/11/05 a joint law enforcement operation known as "Operation Onymous" of American and European law enforcement agencies such as the FBI and Europol led to numerous raids and shut-downs of black markets - including Silk Road 2.0. Figure 1 depicts screenshots of the now-defunct Silk Road 2.0 darknet market and the seizure notification left by the law enforcement agencies.

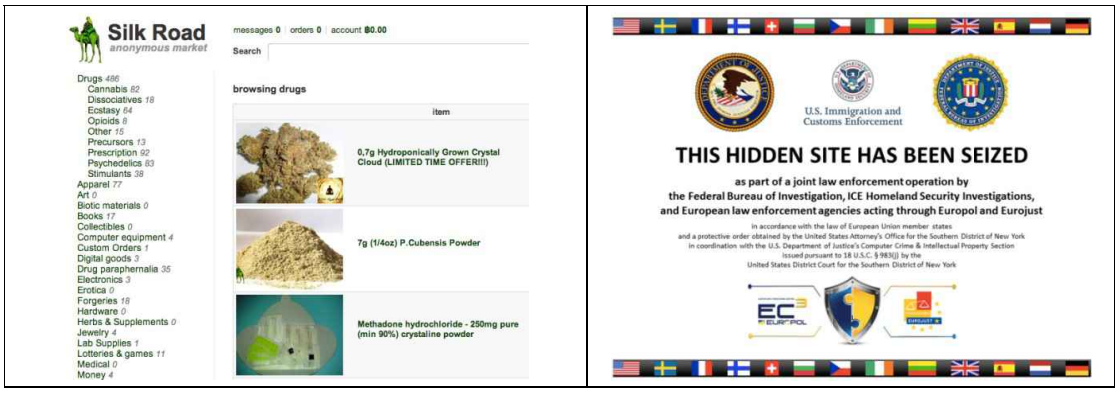

Figure 1. Silk Road 2.0 Interface (Greenberg 2013) and Bust Notification (Greenberg 2014)

Research Model

To study the question whether cryptocurrencies are primarily used as a means of payment in criminal activities, we study the co-evolution of Bitcoin and darknet markets. Specifically, we examine how goods and services sold on darknet markets affect the number of transactions within the Bitcoin blockchain. We do so by explicitly stating and testing two hypotheses.

First, we assume that items sold on darknet markets affect the number of total transactions within the Bitcoin blockchain. Rational choice theory posits that "agents act in their perceived best interest" (Blume and Easley 2008) using a mental cost and benefit calculation prior to decision making (Browning et al. 1999). The aggregate of these individual decisions can be used "to derive hypotheses about the behavior of markets and other systems of economic interest" (Blume and Easley 2008). While the usage of Tor's anonymization capabilities offers a great way to access and operate hidden sites anonymously (Kwon et al. 2015), it was the emergence of the pseudonymous payment system and cryptocurrency Bitcoin (Nakamoto 2008) that solves the second issue in operating a darknet market that protects the true identity of its users: a means of payment which cannot be used by law enforcement agencies to easily trace individuals (Soska and Christin 2015). Based on rational choice theory and the nature of darknet markets, we argue that criminals prefer less over more identifiable ways to buy or sell illicit goods and services. In line with rational choice theory, this is because of decreased costs and increased benefits for both buyers and sellers when compared to more traditional ways of conducting illegal business.

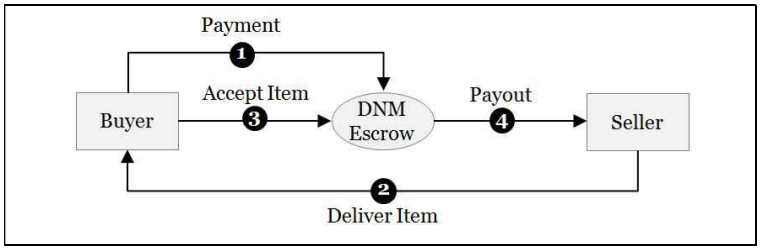

Figure 2. Stylized Darknet Market Escrow Mechanism

Furthermore, we argue that our assumed relationship between items sold on darknet markets and the number of total transactions within the Bitcoin blockchain entails a temporal component. Figure 2 outlines a typical escrow mechanism employed by darknet markets as a means of buyer protection. First, a buyer (B) pays for an item offered by a seller (S). The payment, however, is not paid out directly to S but locked in an escrow account of the darknet marketplace (DNM). Second, S delivers the bought item to B (almost exclusively via mail). Third, the buyer either accepts or declines the item on the DNM. Fourth, based on this decision, the locked amount is paid out to the seller or refunded to the buyer, respectively.

Thus, we assume a time-delayed impact of items sold on darknet markets and the number of transactions within the Bitcoin blockchain. Specifically, we conjecture a time-delayed effect of up to one week. This is because buyers and sellers on darknet markets tend to conduct domestic transactions as strict border controls increases the likelihood of intercepted goods and services in cross-border transaction settings. Domestic transactions with subsequent unlocking of funds held in an escrow mechanism is likely to happen within seven weekdays. We therefore hypothesize:

Hypothesis (H1). *An increased number of goods and services sold on darknet markets is associated with a time-delayed increased number of transactions within the Bitcoin blockchain.*

Second, next to the question whether sales on darknet markets are associated with a time-delayed effect on all transactions within the Bitcoin blockchain, we assume that darknet market providers and darknet market users utilize coin-mixing services to obfuscate their transactions even further. Thus, drawing on the same rational regarding the timing of events from above, we hypothesize that:

Hypothesis (H2). *An increased number of goods and services sold on darknet markets is associated with a time-delayed increased number of Bitcoin blockchain transactions using obfuscation services.*

The reasoning from above is summarized in our research model presented in Figure 3.

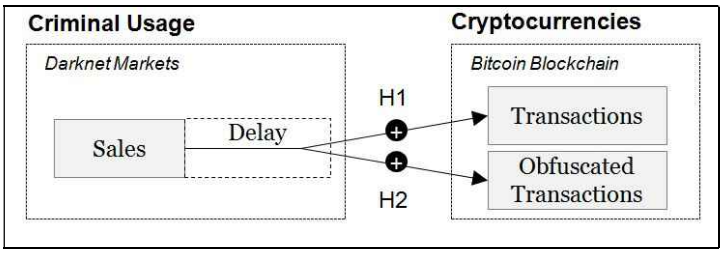

Figure 3. Research Model

Data Set

Within our study, we utilize two data sources. First, we compile daily Bitcoin blockchain transaction data covering the period from June 2014 to July 2015 from Blockchain.info. Specifically, we obtain the total daily number of transactions within the Bitcoin blockchain (*n_tx*), the daily number of transactions excluding long-chains exceeding a length of 10 (*n_tx_ex_lc_10*), 100 (*n_tx_ex_lc_100*), and 1,000 (*n_tx_ex_lc_1000*). Long chain transactions are defined as Bitcoin transactions that are "part of long transaction chains" and likely coin-mixing services (Blockchain.info 2017). We then calculate the number of transactions that are part of long chains exceeding a length of 10 (*n_lc_10)*, 100 (*n_lc_100)*, and 1,000 (*n_lc_1000)* by subtracting *n_tx_ex_lc_10, n_tx_ex_lc_100,* and *n_tx_ex_lc_1000* from *n_tx*.

Second, we draw on a data sample of 296,875 unique product and service listings that were available on nineteen darknet markets from June 2014 to July 2015. The raw data sample was compiled by GRAMS - the preeminent darknet markets search engine. Table 1 provides an overview on the darknet markets included within our analysis. For each market, we report the observation period, the number each market was crawled (#C), the number of unique items (#I) within the observation period, the accepted cryptocurrencies (CCYs) during the observation period, and the market status. Furthermore, we provide the date and reasons on the closure of defunct marketplaces. Here, raid refers to Operation Onymous, exit scam to darknet market operators which disappeared with all funds held in escrow, and voluntarily where the market operators shut down their market by themselves. As of 2016/02/17, 26% of the darknet markets observed were still operating. Out of the 74% of darknet markets which were offline at the same date, a total of 43% were closed due to exit scams, 36% due to raids, 14% because of unknown reasons and 7% due to a voluntarily shut down.

Market	Observation period	# C	# I	CCY	Status (Closure Reason, Date)
Agora	2014/06/09 - 2015/07/12	246	84,322	BTC	Offline (voluntarily, 2015/08/25)
Evolution	2014/06/09 - 2015/03/26	171	75,796	BTC	Offline (exit scam, 2015/03/14)
Silk Road 2.0	2014/06/09 - 2014/11/07	84	24,459	BTC	Offline (raid, 2014/11/05)

AlphaBay	2015/04/04 - 2015/07/12	76	20,037	BTC	* Online (na)
Nucleus Marketplace	2015/02/21 - 2015/07/12	107	19,233	BTC,LTC, DASH	* Online (na)
BlackBank Market	2014/06/09 - 2015/05/21	204	13,702	BTC	Offline (exit scam, 2015/08/18)
Abraxas	2015/04/20 - 2015/07/12	42	10,794	BTC, DASH	Offline (exit scam, 2015/11/06)
Middle Earth Market	2014/07/12 - 2015/07/12	222	10,300	BTC	* Online (na)
Cloud Nine	2014/06/09 - 2014/11/07	93	10,298	BTC	Offline (raid, 2014/11/05)
Pandora	2014/06/09 - 2014/09/03	45	9,254	BTC	Offline (raid, 2014/11/05)
The Onion Market	2014/07/14 - 2014/12/28	45	5,350	BTC	Offline (exit scam, 2014/12/18)
Oxygen	2015/06/09 - 2015/07/12	27	4,306	BTC	Offline (Unknown)
Andromeda	2014/06/09 - 2014/11/19	78	2,403	BTC	Offline (exit scam, 2014/11/18)
Outlaw Market	2014/10/10 - 2015/06/15	143	2,162	BTC	* Online (na)
Silkkitie Market	2015/06/12 - 2015/07/12	24	2,013	BTC	* Online (na)
Pirate Market	2014/06/09 -2014/09/30	75	1,202	BTC	Offline (exit scam, 2014/08/15)
Alpaca Marketplace	2014/08/29 - 2014/11/07	41	658	BTC	Offline (raid, 2014/11/05)
Haven	2015/05/27 - 2015/06/10	12	549	BTC	Offline (unknown)
Bungee54	2014/06/09 - 2014/11/07	95	37	BTC	Offline (raid, 2014/11/05)

Table 1. Darknet Markets Included within the Analysis

For each day t within the observation period, we calculate the aggregate number of goods and services offered on m darknet markets (n_s) by summing up the items offered on each individual darknet market (n_dnm_s) as shown in Equation 1.

$$\text{n\_s}_t = \sum_{m=1}^{19} \text{n\_dnm\_s}_{m,t} \qquad (1)$$

Table 2 provides a summary of our variables used and presents descriptive statistics for the study period from June 2014 to July 2015. All variables are measured on a daily basis. The number of Bitcoin blockchain transactions ranges from 48,515 to 214,487 (SD=23,389.1) with a mean (median) of 90,212.22 (89,437). Transactions that are part of chains longer than 10 range from 30,784 to 150,722 (SD= 16,625.2 with a mean (median) of 60,913.26 (60,423). Thus, a large share of all Bitcoin transactions is part of long chains. A closer examination reveals that on average around 45% of all Bitcoin transactions are part of chains exceeding a length of 100 and 32% a length of 1,000. In addition, it can be observed that the aggregate number of items offered on darknet markets range from 10,282 to 84,376 (SD= 9,598.4) with a mean (median) of 49,600.44 (50,884).

Variable	Description	Period	Min.	Max.	Mean	Median	SD	N
n_tx	No. Bitcoin blockchain transactions	Daily	48,515	214,487	90,212.22	89,437	23,389.1	399
n_lc_10	No. long-chain transactions (>10)	Daily	30,784	150,722	60,913.26	60,423	16,625.2	399
n_lc_100	No. long-chain transactions (>100)	Daily	16,529	122,504	41,488.84	41,701	13,976.2	399
n_lc_1000	No. long-chain transactions (>1,000)	Daily	8,574	104,422	29,756.42	29,267	11,868.9	399
n_s	Aggregate no. items on darknet markets	Daily	10,282	84,376	49,600.44	50,884	9,598.4	399

Table 2. Variables Description and Descriptive Statistics

Methodology

To test our two research hypotheses, we rely on the Autoregressive Distributed Lag (ADL) framework. ADL is considered a "major workhorse in dynamic single-equation regressions" (Hassler and Wolters 2006). Equation 2 presents a general ADL(p,q) model with p lags of the dependent variable Y_t as the autoregressive component and q lags of the independent variable X_t as the distributed lags.

$$\text{ADL}(p,q): \qquad Y_t = \alpha + \sum_{i=1}^{p} \beta_i Y_{t-i} + \sum_{k=0}^{q} \delta_k X_{t-k} + u_t \qquad (2)$$

ADL models require time series data to be stationary. Therefore, we rely on the Augmented Dickey-Fuller (ADF) to test our time series data for stationarity. Table 3 presents results of ADF unit root tests for all five variables before and after first-order differencing. The assumption of non-stationarity could not be rejected for the first four variables before differencing. Therefore, we employ first-order differencing of each time series to stabilize the mean, to remove trends and seasonality (Gido 2010). Note that while this is not required for *n_s*, it enhances the interpretability of the results. Results of the ADF tests on the first-order differenced version of the variables yield a rejection of the null hypothesis "non-stationary" in favor of the alternative, which is "stationary". Note that by calculating the first difference of *n_s*, we also calculated a proxy for darknet market sales. The intuition behind this is that darknet market items are removed from the listings once they are sold.

Before	Variable	n_tx	n_lc_10	n_lc_100	n_lc_1000	n_s
	Statistic	-0.374	-2.216	-1.601	-1.362	-3.702
	P-Value	0.987	0.486	0.746	0.847	0.024 **
After	Variable	Δn_tx	Δn_lc_10	Δn_lc_100	Δn_lc_1000	Δn_s
	Test Statistic	-4.830	-6.913	-6.537	-6.328	-7.999
	P-Value	< 0.01***	< 0.01***	< 0.01***	< 0.01***	< 0.01***

Table 3. Augmented Dickey-Fuller Test Before and After 1st-Order-Differencing

We test H1 by relating changes within the number of transactions on the Bitcoin blockchain to the number of items sold on darknet markets. Specifically, let *t* denote time, Δ*n_tx* first-order differences of the number of transactions within the Bitcoin blockchain and Δ*n_s* the first-order differences of the aggregate number of goods and services offered on darknet markets as a proxy for sales. Furthermore, let *d* denote dummy variables for weekdays and months (coded as 1 if true and 0 otherwise, where one weekday and one month is left out as the reference categories) and *u* the error term, then our first dynamic ADL regression setup can be written as shown in Equation 3.

$$\Delta n\_tx_t = \alpha + \sum_{i=1}^{7} \beta_i \Delta n\_tx_{t-i} + \sum_{k=0}^{7} \delta_i \Delta n\_s_{t-k} + \sum_{n=1}^{17} \theta_n d_{n,t} + u_t \qquad (3)$$

We test H2 by conducting three additional ADL regressions (Equation 4-6). Within Equation 4-6 we draw on the fact that long chain transactions within the Bitcoin blockchain are likely the result of coin-mixing services (Blockchain.info 2017). Specifically, we relate changes in long-chain transactions exceeding a length of 10 (Δn_lc_10), 100 (Δn_lc_100) and 1000 (Δn_lc_1000) to Δ*n_s*. The remaining variables follow the same notation as shown in Equation 3.

$$\Delta n\_lc\_10_t = \alpha + \sum_{i=1}^{7} \beta_i \Delta n\_lc\_10_{t-i} + \sum_{k=0}^{7} \delta_i \Delta n\_s_{t-k} + \sum_{n=1}^{17} \theta_n d_{n.t} + u_t \qquad (4)$$

$$\Delta n\_lc\_100_t = \alpha + \sum_{i=1}^{7} \beta_i \Delta n\_lc\_100_{t-i} + \sum_{k=0}^{7} \delta_i \Delta n\_s_{t-k} + \sum_{n=1}^{17} \theta_n d_{n,t} + u_t \qquad (5)$$

$$\Delta n\_lc\_1000_t = \alpha + \sum_{i=1}^{7} \beta_i \Delta n\_lc\_1000_{t-i} + \sum_{k=0}^{7} \delta_i \Delta n\_s_{t-k} + \sum_{n=1}^{17} \theta_n d_{n,t} + u_t \qquad (6)$$

Empirical Study

Regression Results

Table 4 presents the results of an Ordinary Least Squares (OLS) estimation of the ADL models over 391 days. First, H1 states that an increased number of goods and services sold on darknet markets is associated with a time-delayed increased number of transactions within the Bitcoin blockchain. Looking at the first model (I) we can confirm this hypothesis. We observe a statistically significant effect on the 5% confidence level of the number of goods and services sold on darknet markets six days prior on changes in the number of transactions within the Bitcoin blockchain. Specifically, we show that one additional item sold on darknet markets leads to an increase of 0.123 additional transactions within the Bitcoin

blockchain six days later. This time-lag is in-line with our reasoning regarding the escrow mechanisms with delayed payouts employed by darknet market operators to protect buyers from scams. Furthermore, the effect size can be explained by multiple items bought at once. The model yields an adjusted R^2 of 0.335. Thus, 35.5% of the variance within the outcome variable is explained by the model. Furthermore, the F statistic of 7.145 is statistically significant at the 1% level. Thus, the null hypothesis that every coefficient is zero can be rejected at the 1% level of significance.

	Δn_tx_t-0 (I)	Δn_lc_10_t-0 (II)	Δn_lc_100_t-0 (III)	Δn_lc_1000_t-0 (IV)
Δn_s_t-0	0.063 (0.148)	0.115 (0.137)	0.108 (0.128)	0.079 (0.109)
Δn_s_t-1	0.050 (0.091)	0.049 (0.067)	0.026 (0.071)	0.078 (0.069)
Δn_s_t-2	-0.158 (0.111)	-0.019 (0.066)	0.015 (0.062)	0.001 (0.056)
Δn_s_t-3	0.175 (0.130)	0.026 (0.080)	0.017 (0.073)	-0.004 (0.067)
Δn_s_t-4	-0.084 (0.096)	-0.052 (0.079)	-0.035 (0.072)	-0.012 (0.066)
Δn_s_t-5	0.125 (0.080)	0.049 (0.057)	0.065 (0.057)	0.014 (0.052)
Δn_s_t-6	**0.123**** (0.059)	**0.082*** (0.043)	**0.066*** (0.038)	**0.067*** (0.039)
Δn_s_t-7	0.055 (0.075)	0.035 (0.058)	0.040 (0.050)	0.023 (0.050)
Constant	5,239.448*** (1,480.239)	3,487.633*** (1,124.045)	3,045.618*** (995.230)	2,508.611*** (951.030)
DVAL_t-1 … t-7	Yes	Yes	Yes	Yes
Dummies	Yes	Yes	Yes	Yes
Observations	391	391	391	391
R^2	0.390	0.361	0.286	0.243
Adjusted R^2	0.335	0.304	0.223	0.175
AIC	8,005.6	7,815.2	7,736.7	7,703.6
F Statistic	7.145***	6.330***	4.490***	3.587***

*Notes: Robust Standard Errors in Parentheses. DVAL = Dependent Variable Autoregression Lag. AIC = Akaike Information Criterion. *p<0.1, **p<0.05, ***p<0.01. Dummies: weekday and month.*

Table 4. OLS Estimation of Autoregressive Distributed Lag (ADL) Models (I-IV)

Second, H2 posits that an increased number of goods and services sold on darknet markets is associated with a time-delayed increased number of Bitcoin blockchain transactions using obfuscation services. Looking at model two to four (II - IV) we can confirm this hypothesis as we observe a statistically significant positive effect at the 10% level of darknet market sales on long chain transactions six days later. Following the reasoning on escrow mechanisms from the previous paragraph, we provide an explanation of this time delay. The models (II to IV) yield an adjusted R^2 of 0.361, 0.286 and 0.243 respectively, indicating that the model fit decreases when considering an increased long-chain length. F-values of 6.330 (model II), 4.490 (model III) and 3.587 (model IV) suggest that that the null hypothesis that every coefficient is zero can be rejected at the 1% significance level.

Table 5 presents variable correlation and variance inflation factors. Pearson product-moment correlation coefficients, denoted by Arabic numerals 1-8, reveal moderate correlations among the lagged explanatory variable. Furthermore, Variance Inflation Factors (VIFs), denoted by Roman numerals I-IV, show that our models are not subject to multicollinearity issues. VIFs for time dummies and lagged autoregression terms are not reported but are all below 1.42 and thus provide no indication for multicollinearity issues.

	Pearson-Product Moment Correlation Coefficients								Variance Inflation Factors			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(I)	(II)	(III)	(IV)
(1) Δn_s_t-0	1								1.046	1.047	1.053	1.053
(2) Δn_s_t-1	-0.081	1							1.058	1.062	1.066	1.061
(3) Δn_s_t-2	-0.149	-0.081	1						1.077	1.081	1.084	1.08
(4) Δn_s_t-3	-0.073	-0.153	-0.081	1					1.092	1.09	1.092	1.089
(5) Δn_s_t-4	0.067	-0.072	-0.153	-0.081	1				1.108	1.099	1.101	1.098
(6) Δn_s_t-5	-0.005	0.097	-0.068	-0.174	-0.074	1			1.101	1.101	1.104	1.108
(7) Δn_s_t-6	-0.019	-0.022	0.099	-0.047	-0.178	-0.096	1		1.05	1.05	1.049	1.053
(8) Δn_s_t-7	-0.029	-0.036	-0.021	0.107	-0.047	-0.257	-0.047	1	1.062	1.061	1.06	1.064

Table 5. Variable Correlations and Variance Inflation Factors per Model

Discussion and Limitations

Within our study, we provide evidence for the co-evolution of Bitcoin and darknet markets. Our findings suggest that both, transactions within the Bitcoin blockchain as well as the usage of transaction obfuscation services, can be related to previous sales on darknet markets. We argue that the time lag of six days can be attributed to escrow mechanisms of darknet markets and the effect size on obfuscations services used by darknet market participants. The primary implication of our study is that Bitcoin as the predominant representative for cryptocurrencies seems to be used by criminals to conduct unlawful business. However, the same is true for cash transactions conducted in fiat currencies. Thus, we do not argue for additional regulation of cryptocurrencies because of our finding.

Our study is confronted with several limitations. First, our study focuses on Bitcoin as a proxy for cryptocurrencies. However, Bitcoin paved the way for a large number of so-called altcoins. As of February 2017, more than 600 cryptocurrencies are traded against other (crypto)currencies (Coinmarketcap 2017). Nevertheless, Bitcoin, reaching a current market price of USD 1,038 and a market capitalization of approximately USD 16.7 bn (Coinmarketcap 2017), still dominates the market for cryptocurrencies which yield a total market cap of less than USD 20 bn. Second, we draw on data of nineteen darknet markets as a proxy for organized crime that is associated with cryptocurrency usage. It is possible that our analysis did not capture all relevant criminal usage of cryptocurrencies. However, our darknet market sample appears to be a good approximation for all darknet market activity as it exceeds data of a darknet marketplace watch list by Digital Citizens Alliance (2015). Third, our analysis approximates sales by changes in the daily aggregate supply of goods and services offered on darknet markets. This follows the assumption that offerings are removed once sold. However, darknet market sellers could also remove their listings, e.g. they were sold somewhere else. Like clearnet markets (e.g. Amazon Marketplace), darknet markets hide exact sales figures. Therefore, other sales proxies, such as product reviews, could be used to validate our results. Fourth, darknet markets disappeared and emerged during our observation period, either due to shutdowns or Tor connectivity issues. However, because of how we measure sales, this should not pose an issue for our analysis. When a market shuts down or is not reachable, buying and selling is impossible. Fifth, it is possible that the co-evolution if Bitcoin and darknet markets is especially prevalent in the beginning of both the phenomena of cryptocurrencies and darknet markets. Thus, once cryptocurrencies become more mainstream and the demand for illicit goods and services is met, it is possible that the importance of the co-evolution decreases substantially.

Conclusion

Pseudonymous cryptocurrencies such as Bitcoin are oftentimes associated with illicit activities such as drug trafficking and arms trade. That is, public and private entities routinely deny the utility of privacy preserving means of electronic payments for individuals other than criminals (EUROPOL 2015; Fagan 2013; Honig 2013; Manchin III 2014; Mihm 2013). However, as these discussions are largely based on anecdotal evidence, this paper examines the overall research question of whether pseudonymous cryptocurrencies are primarily used by criminals as a means of payment.

We draw on Rational Choice Theory and the design of darknet markets to build a dynamic research model. Utilizing panel data regarding 296,875 unique product and service listings that were available on nineteen Tor hidden darknet markets from June 2014 to July 2015 as well as Bitcoin blockchain transaction data, we put two research hypotheses to test. We find indications for a co-evolution of Bitcoin and darknet markets. Specifically, our findings suggest that both transactions within the Bitcoin blockchain as well as the usage of transaction obfuscation services can be related to previous sales on darknet markets. We argue that the temporal delay of six days can be attributed to escrow mechanisms of darknet markets and the effect size on obfuscations services used by darknet market participants.

From a theoretical perspective, our study provides first empirical evidence on the co-evolution of Bitcoin and darknet markets as two emergent phenomena in information systems research. Thus, we contribute to the research stream of cryptocurrency usage behavior. From a practical perspective, our results contribute to ongoing discussions of regulators as well as governments concerning the nature of cryptocurrencies and financial services firms considering the usage of cryptocurrencies.

Future work in this area could investigate whether and how the value of goods and services sold on darknet markets are associated with the total value of cryptocurrency transactions within the underlying blockchains and the value of cryptocurrencies itself.

REFERENCES

Ali, S. T., Clarke, D., and McCorry, P. 2015. "Bitcoin: Perils of an Unregulated Global P2P Currency," Springer (available at http://link.springer.com/chapter/10.1007/978-3-319-26096-9_29).

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., and Capkun, S. 2013. "Evaluating user privacy in bitcoin," Financial Cryptography and Data Security, Lecture Notes in Computer Science, pp. 34–51.

Bitlegal.io. 2016. "BitLegal - List," February 22 (available at http://bitlegal.io/list.php; retrieved February 22, 2016).

Blockchain.info. 2017. "Number Of Transactions Excluding Chains Longer Than 10," (available at https://blockchain.info/charts/n-transactions-excluding-chains-longer-than-10; retrieved February 16, 2017).

Blume, L. E., and Easley, D. 2008. "rationality," in The New Palgrave Dictionary of Economics, S. N. Durlauf and L. E. Blume (eds.), (2nd ed.), Basingstoke: Nature Publishing Group, pp. 884–893 (doi: 10.1057/9780230226203.1390).

Browning, G., Halcli, A., and Webster, F. 1999. Understanding Contemporary Society: Theories of the Present, SAGE.

CCN.LA. 2015. "Top 10 Countries in Which Bitcoin is Banned," CCN: Financial Bitcoin & Cryptocurrency News, May 27 (available at https://www.cryptocoinsnews.com/top-10-countries-bitcoin-banned/; retrieved March 3, 2016).

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, International World Wide Web Conferences Steering Committee, pp. 213–224 (available at http://dl.acm.org/citation.cfm?id=2488408).

Coinmarketcap. 2017. "Crypto-Currency Market Capitalizations," February 17 (available at https://coinmarketcap.com/; retrieved February 17, 2017).

Darknetmarkets.org. 2015. "Darknet Markets | A Simple Guide to Safely and Effectively Tumbling (Mixing) Bitcoins.," July 10 (available at https://darknetmarkets.org/a-simple-guide-to-safely-and-effectively-mixing-bitcoins/; retrieved April 24, 2017).

Digital Citizens Alliance. 2015. "Darknet Marketplace Watch - Monitoring Sales of Illegal Drugs on the Darknet," April 24 (available at http://www.digitalcitizensalliance.org/cac/alliance/content.aspx?page=Darknet; retrieved February 16, 2016).

Dingledine, R., Mathewson, N., and Syverson, P. 2004. "Tor: The second-generation onion router," DTIC Document (available at http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA465464).

EUROPOL. 2015. "The Internet Organised Crime Threat Assessment (IOCTA)," (available at https://www.europol.europa.eu/iocta/2015/resources/iocta-2015.pdf).

Fagan, E. J. 2013. "Why Bitcoin (And Other Cryptocurrencies) Will Inevitably Become Tools Of The Rich, Powerful, and Criminal," Business Insider, December 3 (available at http://www.businessinsider.com/why-bitcoin-and-other-cryptocurrencies-will-inevitably-become-tools-of-the-rich-powerful-and-criminal-2013-12; retrieved February 16, 2016).

Gido, van de V. 2010. "STAT 248: Removal of Trend & Seasonality," (available at https://www.stat.berkeley.edu/~gido/Removal%20of%20Trend%20and%20Seasonality.pdf).

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., and Siering, M. 2014. "Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions," in Proceedings of the Twenty Second European Conference on Information Systems, Tel Aviv.

Greenberg, A. 2013. "'Silk Road 2.0' Launches, Promising A Resurrected Black Market For The Dark Web," Forbes, November 6 (available at http://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/; retrieved February 17, 2016).

Greenberg, A. 2014. "Feds Seize Silk Road 2 in Major Dark Web Drug Bust | WIRED," June 11 (available at http://www.wired.com/2014/11/feds-seize-silk-road-2/; retrieved February 17, 2016).

Gwen. 2015. "Black-market risks - Gwern.net," June 28 (available at http://www.gwern.net/Black-market%20survival#data; retrieved February 17, 2016).

Hassler, U., and Wolters, J. 2006. "Autoregressive Distributed Lag Models and Cointegration," in Modern Econometric Analysis, P. D. O. Hübler and P. D. J. Frohn (eds.), Springer Berlin Heidelberg, pp. 57–72 (doi: 10.1007/3-540-32693-6_5).

Honig, Z. 2013. "Bitcoin ban means one less option for bribing Thai officials," Engadget, July 30 (available at http://www.engadget.com/2013/07/30/thailand-bitcoin-ban/; retrieved February 16, 2016).

Kwon, A., AlSabah, M., Lazar, D., Dacier, M., and Devadas, S. 2015. "Circuit fingerprinting attacks: passive deanonymization of tor hidden services," in 24th USENIX Security Symposium (USENIX Security 15), pp. 287–302 (available at https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/kwon).

Manchin III, J. 2014. "Manchin Demands Federal Regulators Ban Bitcoin," February 26 (available at http://www.manchin.senate.gov/public/index.cfm/press-releases?ID=237cbd66-6a26-4870-9bcb-20177ae902b0; retrieved February 14, 2017).

Mihm, S. 2013. "Are Bitcoins the Criminal's Best Friend?," BloombergView, November 18 (available at http://www.bloombergview.com/articles/2013-11-18/are-bitcoins-the-criminal-s-best-friend-; retrieved February 16, 2016).

Moser, M., Bohme, R., and Breuker, D. 2013. "An inquiry into money laundering tools in the Bitcoin ecosystem," in eCrime Researchers Summit (eCRS), 2013, Presented at the eCrime Researchers Summit (eCRS), 2013, , September, pp. 1–14 (doi: 10.1109/eCRS.2013.6805780).

Nakamoto, S. 2008. "Bitcoin: A peer-to-peer electronic cash system," Consulted, (1:2012), p. 28.

Pieters, G. C., and Vivanco, S. 2015. "Bitcoin: A hub of criminal activity?," Available at SSRN 2576452 (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2576452).

Ruffing, T., Moreno-Sanchez, P., and Kate, A. 2014. "CoinShuffle: Practical decentralized coin mixing for Bitcoin," in Computer Security-ESORICS 2014, Springer, pp. 345–364 (available at http://link.springer.com/10.1007/978-3-319-11212-1_20).

Soska, K., and Christin, N. 2015. "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem," in 24th USENIX Security Symposium (USENIX Security 15), pp. 33–48 (available at https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/soska).

Thompson, C. 2013. "The Darkest Place on the Internet Isn't Just for Criminals," WIRED, October 18 (available at http://www.wired.com/2013/10/thompson/; retrieved February 16, 2016).

U.S. Attorney's Office. 2015. "Ross Ulbricht, aka Dread Pirate Roberts, Sentenced in Manhattan Federal Court to Life in Prison," Federal Bureau of Investigation, Press Release, , May 29 (available at https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison; retrieved February 17, 2017).

Yelowitz, A., and Wilson, M. 2015. "Characteristics of Bitcoin users: an analysis of Google search data," Applied Economics Letters, (22:13), pp. 1030–1036.