Finance Research Letters 67 (2024) 105875

Contents lists available at ScienceDirect

Finance Research Letters

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

Dark web traffic, privacy coins, and cryptocurrency trading activity

Stefan Scharnowski

University of Mannheim, L9, 1-2, 68161 Mannheim, Germany

ARTICLE INFO

JEL classification:
G10
G12
G15

Keywords:
Cryptocurrency
Dark web
Trading activity
Privacy coin

ABSTRACT

Cryptocurrencies, especially privacy coins, conceal the flow of money. Similarly, the dark web obscures the flow of internet traffic, increasing anonymity. In this paper, I provide evidence that secondary market trading activity in privacy coins is linked to dark web traffic, although their pricing remains mostly unaffected. This finding holds after considering various controls and comparing similar privacy and non-privacy coins. However, when disentangling dark web traffic by country of origin, I find that privacy coin prices correlate positively with traffic from China, while trading volume is mainly driven by users from Russia and Iran.

1. Introduction

The advent of cryptocurrencies has provided a layer of anonymity to financial transactions, complicating the efforts to monitor and regulate digital marketplaces and international money flows. Illicit uses of cryptocurrencies broadly fall into five categories, with some overlap: circumvention of capital controls, money laundering and tax evasion, payments for illegal goods and services, cybercrimes (such as ransomware and extortion), and terrorism financing. While conventional cryptocurrencies such as Bitcoin have been – and still are – used for these purposes, they are pseudonymous and relatively transparent due to their publicly accessible transaction history on their respective blockchains. For this reason, privacy coins such as Monero (XMR), Zcash (ZEC), and Dash (DASH) stand out for their enhanced anonymity features, obscuring transactions and thus making them preferred choices for illegal activity.

Privacy coins obfuscate the flow of funds. Similarly, the dark web obfuscates the flow of internet traffic. It hosts a variety of legal and illegal activities. While it facilitates encrypted communications for journalists, whistleblowers, and individuals within authoritarian regimes, it is notorious for its association with illegal endeavors, including the distribution of narcotics, weapons, stolen data, and counterfeit currency. Additionally, it serves as a haven for illicit services such as fraud, cybercrime, human trafficking, and illegal pornographic material. The inherent anonymity provided by the dark web complicates the efforts of global law enforcement agencies in detecting and mitigating criminal activities within this obscured part of the internet (Cronin, 2018).

In this paper, I explore the relationship between dark web traffic and cryptocurrency trading activity in the secondary market, with a particular focus on privacy coins. There are several reasons to expect such a relationship. Accessing dark web marketplaces (often referred to as darknet markets, or DNMs) and paying for goods and services purchased there would lead to a correlation between dark web traffic and privacy coin activity. For example, the now offline DNM White House Market, once among the largest such marketplaces, stopped accepting Bitcoin and shifted to only accepting XMR for payments (Blockchain Council, 2022). Other DNMs accept both non-privacy and privacy coins, with some marketplaces then trading non-privacy for privacy coins and vice versa to launder the money (Chainalysis, 2024). Similarly, trading on cryptocurrency exchanges or using cryptocurrency cash-out services while directing the corresponding internet traffic through the dark web allows users to better hide their identities.

E-mail address: scharnowski@uni-mannheim.de.

https://doi.org/10.1016/j.frl.2024.105875
Received 20 March 2024; Received in revised form 9 July 2024; Accepted 14 July 2024
Available online 23 July 2024

Moreover, government restrictions on capital flows often coincide with other restrictions which may make their citizens more reliant on concealing their internet activity. Understanding this relationship is important, as it sheds light on the dynamics of potentially illicit online activity and provides insights into the challenges faced by regulators and law enforcement agencies.

I find that – relative to other cryptocurrencies – trading activity in privacy coins is positively associated with the number of users connecting to the dark web. However, privacy coin prices appear to be mostly unaffected. The results are robust to including several control variables and when applying a matching procedure to compare otherwise similar privacy and non-privacy coins. When splitting dark web traffic into its countries of origin, I find a positive relationship between dark web traffic from China and the relative prices of privacy coins. Trading activity, on the other hand, appears to be mostly driven by dark web activity from Russia and Iran. While the nature of the dark web and of privacy coins make it difficult to ascertain what exactly a given cryptocurrency transaction relates to, the overall results are consistent with privacy coins being used not only to pay for illegal purchases on DNMs, but also to circumvent government restrictions and sanctions.

The paper contributes to multiple streams in the literature. Firstly, it adds to the literature on the usage of cryptocurrencies, in particular with respect to illicit activities. In this stream, Foley et al. (2019) estimate that a significant portion of about 25% of Bitcoin users are involved in illicit activities. Furthermore, this number is inversely related to the market capitalization of privacy coins (called *shadow coins* in their paper). Almaqableh et al. (2023) analyze the effects of drug busts on cryptocurrency markets and find evidence that links drug trafficking and cryptocurrency markets. Jawaheri et al. (2020) present ways of deanonymizing dark web users through Bitcoin transactions, pointing to privacy risks associated with the currency. Moreover, several studies investigate how cryptocurrencies are used to evade capital controls and government restrictions (Hu et al., 2023; Alnasaa et al., 2022; Roche et al., 2023).

Privacy coins address the transparency of conventional cryptocurrencies but have received substantially less academic attention. In this stream, Sapkota and Grobys (2021) find that privacy coins constitute a distinct market equilibrium separate from non-privacy cryptocurrencies which might arise from their appeal to users seeking anonymity, possibly for criminal activities. Bahamazava and Nanda (2022) investigate the migration from Bitcoin to more privacy-centric cryptocurrencies within darknet markets, highlighting a trend towards anonymity. Hilmola (2021) observes that privacy coins have struggled to maintain their value relative to Bitcoin. However, there is very little academic evidence on secondary market trading activity in privacy coins.

This study further contributes to the literature on the determinants of cryptocurrency trading activity. Aalborg et al. (2019) find that Bitcoin's trading volume is significantly influenced by network-specific factors like the number of unique addresses used in transactions and market sentiment. Brauneis et al. (2020) and Scharnowski (2021) corroborate these findings, highlighting that cryptocurrency-specific factors drive cryptocurrency liquidity. Brauneis et al. (2024) show that cryptocurrency liquidity and trading activity co-moves substantially across different exchanges and currency pairs. Still, the literature on the determinants of trading activity in privacy coins is scarce. In this paper, I attempt to fill this gap.

2. Empirical approach

2.1. Data

The data ranges from January 2017 until December 2023 and comes from two sources. Firstly, to measure dark web traffic, I rely on estimates of the daily number of users connecting to the Tor network via bridges from the Tor Project.[1] Tor, or "The Onion Router", is a network designed for anonymous and secure access to the internet, typically via the Tor Browser. Network traffic is layered and encrypted, hiding the user's path. The network consists of volunteer-operated servers, including entry nodes (knowing the origin of a user's internet traffic but not the destination), middle nodes (transferring data anonymously), and exit nodes (knowing the destination but not the origin). Tor bridges are special nodes that are not listed in the public directory of Tor nodes, adding an additional layer of protection and censorship resistance (The Tor Project, 2024). While not all traffic in the network is related to illegal activity, prior studies have documented that it is often used for illicit activity such as dealing drugs, human trafficking, and cybercrimes (Cronin, 2018; Duxbury and Haynie, 2018; Meland et al., 2020).

Secondly, I collect trading data on 13 cryptocurrencies from the centralized cryptocurrency exchange Kraken, which is generally considered trustworthy.[2] The sample contains ten non-privacy coins and the three privacy coins actively traded at Kraken: Dash, Monero, and Z-Cash. These privacy coins capture the majority of trading activity in the privacy coin market and have been actively traded for several years. The data contains daily closing prices, trading volume, and the number of trades. I calculate log returns based on prices C_t as

$$r_t = \ln\left(\frac{C_t}{C_{t-1}}\right) \tag{1}$$

and estimate daily volatility using the asymmetric GJR-GARCH(1,1) model.[3]

To analyze the impact of dark web traffic on privacy coins, I estimate variations of the following panel regression model

$$y_{i,t} = \ \alpha + \beta_1 \text{DarkTraffic}_t + \beta_2 \text{PrivacyCoin}_i + \ \beta_3 \text{DarkTraffic}_t \times \text{PrivacyCoin}_i + \beta_4 \text{Controls}_{i,t} + \varepsilon_{i,t} \tag{2}$$

[1] https://metrics.torproject.org

[2] The sample was selected as follows: The 50 largest files containing historical daily OHLC data of non-stablecoin cryptocurrencies trading against the US dollar were collected from Kraken. Next, least 2000 observations per cryptocurrency were required.

[3] I obtain very similar results when using other GARCH models or when estimating volatility by the absolute value of daily returns.

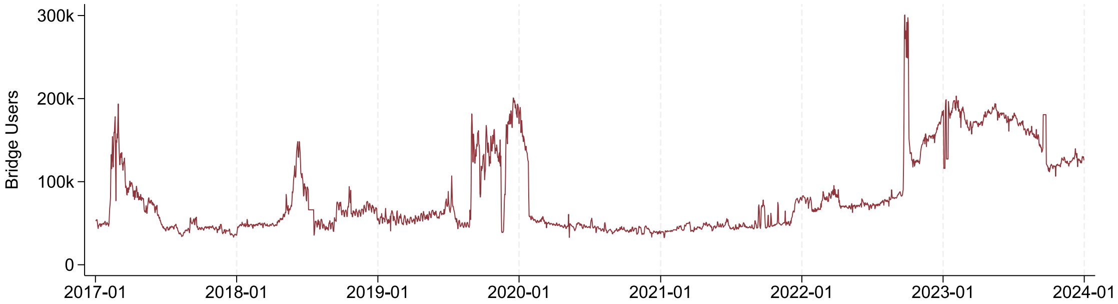

Fig. 1. Tor bridge users. This graph shows the development of the estimated number of daily users connecting to the Tor network via bridges.

Table 1
Summary Statistics.

Ticker	Privacy	Return			Volume			Trades			N	First
		Mean	SD	P50	Mean	SD	P50	Mean	SD	P50		
BCH	–	−0.01	6.43	−0.04	3.16	5.63	1.43	3.30	3.67	2.12	2343	2017–08-01
BTC	–	0.15	3.95	0.12	86.46	98.46	55.37	25.49	19.34	21.49	2555	2017–01-02
DASH	✓	−0.03	5.84	0.02	0.55	1.31	0.20	1.06	1.47	0.57	2454	2017–04-12
EOS	–	−0.02	7.41	0.00	1.37	3.21	0.55	1.63	2.33	0.91	2374	2017–07-01
ETC	–	0.11	6.24	−0.08	1.02	5.95	0.26	1.51	2.94	0.73	2555	2017–01-02
ETH	–	0.22	5.20	0.10	55.30	81.89	26.32	18.12	16.98	13.72	2555	2017–01-02
GNO	–	0.04	5.27	0.00	0.05	0.14	0.01	0.21	0.28	0.12	2435	2017–05-01
LTC	–	0.11	5.72	−0.02	4.29	7.59	1.85	4.24	4.18	3.10	2555	2017–01-02
REP	–	−0.02	6.65	0.00	0.09	0.19	0.03	0.33	0.52	0.15	2555	2017–01-02
XLM	–	0.16	8.69	0.00	1.44	3.63	0.44	2.08	3.30	1.13	2539	2017–01-17
XMR	✓	0.09	5.44	0.13	1.32	1.90	0.67	1.90	1.76	1.43	2554	2017–01-02
XRP	–	0.02	6.22	−0.04	8.57	16.26	3.55	6.18	8.48	3.65	2418	2017–05-18
ZEC	✓	−0.02	6.02	0.05	0.80	1.99	0.23	1.20	1.62	0.67	2555	2017–01-02

This table shows summary statistics for the sample cryptocurrencies using trading data from the exchange Kraken. *Privacy* indicates privacy coins. *Return* is the logarithmic return based on daily closing prices and given in percentage points. *Volume* is the daily trading volume in USD 1mn. *Trades* is the number of daily trades in 1000. *First* shows the date of the first observation in the sample.

where $y_{i,t}$ is either returns, trading volume, or the number of trades of cryptocurrency i on date t, *DarkTraffic* is the number of users connecting to the Tor network via bridges, *Privacy* is a binary variable indicating privacy coins and *Controls* is a vector of control variables containing the price and volatility of a cryptocurrency as well as cryptocurrency and date fixed effects. Standard errors are clustered by cryptocurrency.[4]

3. Empirical analysis

3.1. Summary statistics

The number of bridge users in the Tor network varies substantially over time. Fig. 1 shows its development. Notably, there are several spikes in dark web activity, for example towards the end of 2021 and in October 2023. Moreover, in 2023, there is generally a high level of dark web traffic, while during most of 2020 and 2021 it was relatively low.

Summary statistics can be found in Table 1. Overall, privacy and non-privacy coins have comparable levels of returns at a similar level of volatility. Trading activity is on average lower in the privacy coins. Especially the more established cryptocurrencies Bitcoin (BTC) and Ether (ETH) are much more actively traded.

3.2. Dark web traffic and privacy coin activity

I first investigate how dark web traffic is related to the pricing of privacy coins. In the baseline model (1) in Table 2, the coefficient for dark web traffic is negative and significant, but the effect disappears when controlling for the price level and volatility in model (2). The coefficient for privacy coins is insignificant, indicating that privacy coins are not generally exhibiting different returns than non-privacy coins. The coefficient for the interaction of dark web traffic and privacy coins, while positive, is statistically insignificant. This holds for all specifications, including the one with fixed effects in model (3). Overall, the results do not provide evidence that

[4] Note that due to the small number of clusters, critical values are based on the t distribution with $G-1$ degrees of freedom, where G is the number of clusters (see e.g. Cameron and Miller, 2015).

Table 2
Returns.

	(1)	(2)	(3)
DarkTraffic	−0.654**	0.034	
	(−2.63)	(0.09)	
PrivacyCoin	−0.085	−0.086	
	(−1.25)	(−1.25)	
PrivacyCoin × DarkTraffic	0.236	0.733	0.361
	(0.62)	(1.58)	(0.63)
Price		0.008***	−0.003
		(3.41)	(−1.65)
Volatility		0.064**	0.023
		(2.58)	(0.64)
Coin FE	–	–	✓
Date FE	–	–	✓
Adj. R^2	−0.00	0.00	0.52
N	32,447	32,447	32,447

This table shows panel regression results for daily log returns based on closing prices in percentage points.
DarkTraffic is the estimated number of users connecting via Tor bridges. PrivacyCoin is a binary variable indicating privacy coins. Price is the daily closing price of a given cryptocurrency in USD. Volatility is the estimated daily standard deviation of log returns in percentage points. Standard errors are clustered by cryptocurrency and *t*-statistics reported in parentheses. ***, **, * denotes significance at the 1%, 5%, 10%–level, respectively.

Table 3
Trading Activity.

	Trading Volume			# Trades		
	(1)	(2)	(3)	(4)	(5)	(6)
DarkTraffic	−69.858*	−74.899*		−20.244**	−19.810**	
	(−2.10)	(−1.89)		(−3.05)	(−2.58)	
PrivacyCoin	−20.744	−13.363		−6.003*	−4.359*	
	(−1.71)	(−1.75)		(−1.94)	(−1.90)	
PrivacyCoin × DarkTraffic	62.798*	75.782*	74.646*	12.145*	16.164**	16.664*
	(1.89)	(1.91)	(1.93)	(1.81)	(2.31)	(2.14)
Price		4.142***	3.640***		0.941***	0.543***
		(26.73)	(18.15)		(15.91)	(17.05)
Volatility		0.249	0.343		0.201	0.423**
		(0.48)	(0.75)		(1.00)	(2.22)
Coin FE	–	–	✓	–	–	✓
Date FE	–	–	✓	–	–	✓
Adj. R^2	0.03	0.42	0.55	0.04	0.38	0.65
N	32,454	32,454	32,454	32,454	32,454	32,454

This table shows panel regression results for trading activity. In columns (1)–(3), the dependent variable is the trading volume in USD 1mn. In columns (4)–(6), the dependent variable is the number of trades in 1000.
DarkTraffic is the estimated number of users connecting via Tor bridges. PrivacyCoin is a binary variable indicating privacy coins. Price is the daily closing price of a given cryptocurrency in USD. Volatility is the estimated daily standard deviation of log returns in percentage points. Standard errors are clustered by cryptocurrency and *t*-statistics reported in parentheses. ***, **, * denotes significance at the 1%, 5%, 10%–level, respectively.

dark web traffic impacts privacy coin prices on average. However, note that unaffected average prices do not necessarily imply that dark web traffic is not related to changes in privacy coin demand. A possible explanation for the insignificant effect could be that the effects of dark web related buys and sells cancel out. I hence look at the effect of dark web traffic on trading activity, which does not suffer from this drawback.

The results in Table 3 show that while dark web traffic is generally associated with lower trading activity in cryptocurrencies, the same does not hold for privacy coins. The coefficient for the interaction term is positive and significant for both trading volume (models 1–3) and the number of trades when controlling for price levels and volatility (models 5–6). The effect is robust to the inclusion of fixed effects. This suggests that there is a relationship between dark web traffic and secondary market trading activity, consistent with the notion that privacy coins are more frequently used for illicit purposes such as paying for illegal goods and services or circumventing capital controls and government sanctions than conventional cryptocurrencies. However, the approach does not allow for drawing further conclusions regarding the nature of this relationship. I reconsider this issue in Section 3.4.

Table 4
Matched Sample.

	Returns			Trading Volume			# Trades		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
DarkTraffic	−1.110**	−0.546		−11.682***	−9.856**		−11.519***	−9.803***	
	(−2.70)	(−0.90)		(−8.04)	(−3.77)		(−11.66)	(−6.66)	
PrivacyCoin	−0.131	−0.414**		−0.755*	−1.417***		−0.636**	−1.222**	
	(−1.55)	(−3.98)		(−2.49)	(−5.47)		(−2.57)	(−3.88)	
PrivacyCoin × DarkTraffic	0.692	2.933*	1.289	4.622**	10.860***	7.695***	3.420*	9.144**	6.319**
	(1.35)	(2.51)	(1.16)	(3.06)	(5.91)	(4.93)	(2.34)	(3.75)	(3.15)
Price		1.722**	−0.023		4.270	0.866		3.833	1.292
		(3.60)	(−0.05)		(1.55)	(1.06)		(1.55)	(0.97)
Volatility		0.077	0.059		0.250*	0.223		0.236**	0.171*
		(1.51)	(0.85)		(2.15)	(1.77)		(3.11)	(2.47)
Matching	✓	✓	✓	✓	✓	✓	✓	✓	✓
Coin FE	–	–	✓	–	–	✓	–	–	✓
Date FE	–	–	✓	–	–	✓	–	–	✓
Adj. R^2	−0.00	0.00	0.52	0.02	0.07	0.35	0.05	0.13	0.49
N	15,031	15,031	15,031	15,035	15,035	15,035	15,035	15,035	15,035

This table shows panel regression results similar to Table 2 and Table 3 but when using a matched sample of non-privacy coins. The matching is performed on average values of returns, trading volume, and the number of trades.
DarkTraffic is the estimated number of users connecting via Tor bridges. PrivacyCoin is a binary variable indicating privacy coins. Price is the daily closing price of a given cryptocurrency in USD. Volatility is the estimated daily standard deviation of log returns in percentage points. Standard errors are clustered by cryptocurrency and t-statistics reported in parentheses. ***, **, * denotes significance at the 1%, 5%, 10%–level, respectively.

3.3. Matching approach

A concern regarding the analysis may be that the sample of privacy coins differs in important aspects other than privacy features. In particular, the average non-privacy coin has a higher level of trading activity and market capitalization. To address this, I match an observationally similar non-privacy coin to each privacy coin. The matching is performed without replacement and based on average returns, trading volume, and number of trades using an adjusted version of the metric of Huang and Stoll (1996)

$$j_i^* = \underset{j}{\operatorname{argmin}} \left[\left(\frac{\bar{r}_i - \bar{r}_j}{\bar{r}_i + \bar{r}_j} \right)^2 + \left(\frac{\overline{Vol}_i - \overline{Vol}_j}{\overline{Vol}_i + \overline{Vol}_j} \right)^2 + \left(\frac{\overline{Trades}_i - \overline{Trades}_j}{\overline{Trades}_i + \overline{Trades}_j} \right)^2 \right] \tag{3}$$

where i indexes privacy coins and j indexes non-privacy coins.[5]

The matched sample consists of Ethereum Classic (ETC), Stellar Lumen (XLM), and EOS. The regression results based on this sample are shown in Table 4 and generally confirm the previous findings. Compared to the matched sample of non-privacy coins, trading activity in privacy coins is higher when dark web traffic is high. Prices are generally not strongly impacted. In model (2), the effect of dark web traffic on privacy coin returns is positive and significant, but the effect disappears when including fixed effects.

3.4. Country level analysis

The previous analyses investigate the effect of *global* dark web traffic. I now disentangle dark web traffic by country based on the geolocation of IP addresses of incoming traffic. This data is also provided by the Tor project. While not perfectly accurate, for example because some dark web users may take additional steps in cloaking their origin by first connecting through private tunnels, this approach still provides a proxy for the traffic originating in a given country.

The countries with the most daily average users connecting via bridges are (in descending order): Russia, Iran, the United States, the United Arab Emirates, Germany, China, the United Kingdom, India, Turkey, France. The time series of bridge users for some countries are highly correlated, especially for the European countries. To avoid multicollinearity, I hence focus on the most relevant countries and combine the remaining countries.[6]

The first column in Table 5 shows the results for returns. While most coefficients are statistically insignificant, the effect of dark web traffic originating in China on privacy coin prices relative to the prices of other cryptocurrencies is positive and both statistically and economically significant. This suggests that, while global dark web traffic on average does not influence privacy coin prices, users connecting from China do have a positive influence. A potential explanation for this finding could be that some traders located in China purchase these coins to circumvent capital controls but do not immediately sell them in another market, thus increasing demand and prices of privacy coins.

[5] The matched sample and thus the results are identical when matching only on trading volume and the number of trades.

[6] In particular, the considered individual countries are Russia, Iran, the United States, the United Arab Emirates, and China, while traffic originating from other countries is included as a joint variable. When specified in this way, the average variance inflation factor is 3.29 with a maximum value of 5.98 and thus unproblematic. Further disentangling dark web traffic results in substantially higher variance inflation factors, making it unlikely that the effects of traffic from different origin countries can be meaningfully separated.

Table 5
Country Level Analysis.

	Returns	Trading Volume	# Trades
PrivacyCoin × $\text{DarkTraffic}_{\text{Russia}}$	3.946	42.239***	29.496*
	(0.65)	(4.28)	(2.56)
PrivacyCoin × $\text{DarkTraffic}_{\text{Iran}}$	1.751	7.327***	7.495***
	(0.70)	(5.78)	(4.77)
PrivacyCoin × $\text{DarkTraffic}_{\text{US}}$	−12.688	−39.184	−17.324
	(−0.86)	(−1.73)	(−0.71)
PrivacyCoin × $\text{DarkTraffic}_{\text{UAE}}$	2.342	16.720*	9.344
	(0.34)	(2.34)	(0.80)
PrivacyCoin × $\text{DarkTraffic}_{\text{China}}$	133.863**	149.293	96.811
	(3.68)	(1.54)	(1.01)
PrivacyCoin × $\text{DarkTraffic}_{\text{Rest}}$	−5.123	−17.930	−20.844
	(−1.02)	(−1.05)	(−1.09)
Price	0.133	1.225	1.542
	(0.30)	(1.61)	(1.15)
Volatility	0.060	0.226	0.174*
	(0.86)	(1.79)	(2.42)
Matching	✓	✓	✓
Coin FE	✓	✓	✓
Date FE	✓	✓	✓
Adj. R^2	0.52	0.35	0.49
N	15,031	15,035	15,035

This table shows panel regression results similar to Table 2 and Table 3 but when using a matched sample of non-privacy coins. The matching is performed on average values of returns, trading volume, and the number of trades.

DarkTraffic is the estimated number of users connecting via Tor bridges. PrivacyCoin is a binary variable indicating privacy coins. Price is the daily closing price of a given cryptocurrency in USD. Volatility is the estimated daily standard deviation of log returns in percentage points. Standard errors are clustered by cryptocurrency and t-statistics reported in parentheses. ***, **, * denotes significance at the 1%, 5%, 10%–level, respectively.

Trading activity, in contrast, appears to be driven by users connecting from Russia, Iran, and the United Arab Emirates. For trading volume in privacy coins, the effect of dark web traffic from all three countries is positive and significant. For the number of trades, only traffic originating from Russia and Iran shows a significant relationship. While this analysis does not provide direct evidence regarding the exact usages of privacy coins, it seems likely that privacy coins are used for different purposes across these countries. For example, several large DNMs are linked to Russia, such as the now closed Hydra market. DNMs seeking to take Hydra's place such as Mega Darknet or Kraken Market[7] are also linked to Russia (see also Chainalysis, 2024). Conversely, in the case of Iran, cryptocurrencies are likely rather used to circumvent sanctions and capital controls.

3.5. *Further robustness tests*

Another concern might be the choice of trading venue. While Kraken is a highly liquid exchange, there are exchanges with more lenient Know Your Customer (KYC) and Anti-money Laundering (AML) procedures. In particular, the centralized exchange Binance has admitted to "failing to maintain an effective anti-money laundering [. . .] program" (U.S. Department of Justice, 2023). According to Secretary of the Treasury Janet L. Yellen, Binance's "willful failures allowed money to flow to terrorists, cybercriminals, and child abusers" (U.S. Department of Justice, 2023). However, privacy coin trading began substantially later at Binance than at Kraken. Privacy coin data becomes available starting March 2019, resulting in a significantly smaller sample. Still, I repeat the matched sample and country level analyses using this data. The results are overall very similar.[8]

To further establish robustness, in untabulated analyses I confirm that the results are robust to including lagged values of the dependent variables in the regressions. Moreover, winsorizing all variables at the 99% level does not materially change the conclusions.

[7] Not to be confused with Kraken, the cryptocurrency exchange.

[8] In particular, relative trading activity in privacy coins still increases significantly in dark web traffic while returns are mostly unaffected. The country level results generally become stronger. The most important differences when using Binance data are that dark web traffic from China is significantly positively associated with both privacy coin prices and trading activity. Moreover, the impact of dark web traffic from the UAE increases while traffic originating from Iran becomes less statistically significant. For brevity, the results are available upon request. On February 20th, 2024, Binance announced the delisting of XMR due to regulatory compliance concerns. I also note that an alternative to regular exchanges can be found in instant exchangers: Centrally-managed but non-custodial crypto-to-crypto exchanges that specialize in trading privacy coins such as XMR (Chainalysis, 2024).

4. Concluding remarks

In this study, I analyze the relationship between dark web traffic and the market dynamics of privacy coins. I find that while global dark web traffic does not significantly impact the prices of privacy coins, they are influenced by traffic originating in China. Moreover, there is a positive effect of dark web activity on trading volume, mostly driven by traffic from Russia and Iran. The findings suggest that privacy coins are utilized differently across different geopolitical landscapes. On the one hand, the findings are consistent with the notion that privacy coins are used on dark web marketplaces to pay for illicit goods and services such as drugs or ransomware attacks. On the other hand, they are also likely used to circumvent capital controls or international sanctions. The analysis has significant implications for policymakers and law enforcement, pointing to the need for targeted approaches to monitor and regulate the use of privacy coins.

My approach likely underestimates the extent to which privacy coins and the dark web are related. For example, throughout the paper I focus on contemporaneous effects, while secondary market activity could also lead or lag behind dark web activity. Moreover, to measure trading activity, I focus on a centralized exchanges, while those using cryptocurrencies for illicit purposes presumably also use decentralized exchanges. The results should hence be understood as a lower bound of the effect of dark web activity on cryptocurrency trading activity.

CRediT authorship contribution statement

Stefan Scharnowski: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Resources, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization.

Data availability

Data will be made available on request.

References

Aalborg, H.A., Molnár, P., de Vries, J.E., 2019. What can explain the price, volatility and trading volume of Bitcoin? Finance Res. Lett. 29, 255–265. http://dx.doi.org/10.1016/j.frl.2018.08.010.

Almaqableh, L., Wallace, D., Pereira, V., Ramiah, V., Wood, G., Veron, J.F., Moosa, I., Watson, A., 2023. Is it possible to establish the link between drug busts and the cryptocurrency market? Yes, we can. Int. J. Inf. Manage. 71, 102488. http://dx.doi.org/10.1016/j.ijinfomgt.2022.102488.

Alnasaa, M., Gueorguiev, N., Honda, J., Imamoglu, E., Mauro, P., Primus, K., Rozhkov, D., 2022. Crypto-assets, corruption, and capital controls: Cross-country correlations. Econom. Lett. 215, 110492. http://dx.doi.org/10.1016/j.econlet.2022.110492.

Bahamazava, K., Nanda, R., 2022. The shift of DarkNet illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence. Forensic Sci. Int.: Digit. Invest. 40, 301377. http://dx.doi.org/10.1016/j.fsidi.2022.301377.

Blockchain Council, 2022. Darknet Analysis On Hydra And Other Markets Reveals Interesting Facts. URL: https://www.blockchain-council.org/blockchain/darknet-analysis-on-hydra-and-other-markets-reveals-interesting-facts/.

Brauneis, A., Mestel, R., Theissen, E., 2020. What drives the liquidity of cryptocurrencies? A long-term analysis. Finance Res. Lett. 101537. http://dx.doi.org/10.1016/j.frl.2020.101537.

Brauneis, A., Mestel, R., Theissen, E., 2024. The crypto world trades at tea time: intraday evidence from centralized exchanges across the globe. Rev. Quant. Financ. Account. http://dx.doi.org/10.1007/s11156-024-01304-1.

Cameron, A.C., Miller, D.L., 2015. A practitioner's guide to cluster-robust inference. J. Hum. Resour. 50 (2), 317–372. http://dx.doi.org/10.3368/jhr.50.2.317.

Chainalysis, 2024. The 2024 Crypto Crime Report. URL: https://go.chainalysis.com/crypto-crime-2024.html.

Cronin, M.J., 2018. Hunting in the dark: A prosecutor's guide to the dark net and cryptocurrencies. Dep. Justice J. Fed. Law Pract. 66 (4), 65–78.

Duxbury, S.W., Haynie, D.L., 2018. The network structure of opioid distribution on a darknet cryptomarket. J. Quant. Criminol. 34 (4), 921–941. http://dx.doi.org/10.1007/s10940-017-9359-4.

Foley, S., Karlsen, J.R., Putnins, T.J., 2019. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? Rev. Financ. Stud. 32 (5), 1798–1853. http://dx.doi.org/10.1093/rfs/hhz015.

Hilmola, O.P., 2021. On prices of privacy coins and bitcoin. J. Risk Financ. Manag. 14 (8), http://dx.doi.org/10.3390/jrfm14080361.

Hu, M., Lee, A.D., Putnins, T.J., 2023. Evading Capital Controls via Cryptocurrencies: Evidence from the Blockchain. (ISSN: 1556-5068) http://dx.doi.org/10.2139/ssrn.3956933, Working Paper.

Huang, R.D., Stoll, H.R., 1996. Dealer versus auction markets: A paired comparison of execution costs on NASDAQ and the NYSE. J. Financ. Econ. 41 (3), 313–357. http://dx.doi.org/10.1016/0304-405X(95)00867-E.

Jawaheri, H.A., Sabah, M.A., Boshmaf, Y., Erbad, A., 2020. Deanonymizing Tor hidden service users through Bitcoin transactions analysis. Comput. Secur. 89, 101684. http://dx.doi.org/10.1016/j.cose.2019.101684, arXiv:1801.07501.

Meland, P.H., Bayoumy, Y.F.F., Sindre, G., 2020. The Ransomware-as-a-Service economy within the darknet. Comput. Secur. 92 (7034), http://dx.doi.org/10.1016/j.cose.2020.101762.

Roche, G.A.G., Noël, A., Sauce, L., 2023. Between Governance and Capital Restrictions: Determinants of Bitcoin Trade Volume in Decentralized Markets. Working Paper. URL: https://ssrn.com/abstract=4409613.

Sapkota, N., Grobys, K., 2021. Asset market equilibria in cryptocurrency markets: Evidence from a study of privacy and non-privacy coins. J. Int. Financ. Mark. Inst. Money 74 (July), 101402. http://dx.doi.org/10.1016/j.intfin.2021.101402.

Scharnowski, S., 2021. Understanding bitcoin liquidity. Finance Res. Lett. 38, 101477. http://dx.doi.org/10.1016/j.frl.2020.101477.

The Tor Project, 2024. What is a bridge? URL: https://support.torproject.org/censorship/censorship-7/.

U.S. Department of Justice, 2023. Binance and CEO Plead Guilty to Federal Charges in $4B Resolution. URL: https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.