Offending concentration on the internet: An exploratory analysis of Bitcoin-related cybercrime

Authors

David Buil-Gil[1] and Patricia Saldaña-Taboada[2]

[1]Department of Criminology, University of Manchester, UK

[2]Criminal Law Department, University of Granada, Spain

Full citation

Buil-Gil, D., and Saldaña-Taboada, P. (2021). Offending concentration on the internet: An exploratory analysis of Bitcoin-related cybercrime. *Deviant Behavior.*

Corresponding author

David Buil-Gil. 2.17 Williamson Building, University of Manchester, Oxford Road, M13 9PL, UK. Email: david.builgil@manchester.ac.uk

Abstract

Crime research has repeatedly shown that small proportions of offenders are responsible for large proportions of crimes. While there is a substantial body of evidence for this 'offending concentration' in connection to traditional offline crime, there is limited research assessing the concentration of offending for cybercrime. This research analyzes victim reports of Bitcoin-related cybercrimes (blackmail, ransomware, sextortion, darknet market fraud, Bitcoin tumbler fraud) to illuminate the extent of cybercrime offending concentration and to identify groups of offenders involved in online crime. Our results indicate that a large proportion of cybercrimes are associated to a small number of very active Bitcoin addresses. However, Bitcoin addresses associated to high numbers of reports are not necessarily those that generate the largest financial benefits.

Keywords

Environmental criminology; Crime analysis; Lorenz curve; Online crime; Blackmail; Sextortion

Introduction

For many decades, criminologists have been aware that disproportionately few offenders are responsible for most crimes, while most people commit very few or even no offences. This 'offending concentration' has been observed across many crime types and geographic contexts (Martinez et al., 2017). Clarke and Eck (2005) argued that the concentration of crime in offenders follows the 80/20 rule, which is also known as the Pareto principle or the power law distribution in mathematics, by which 20% of offenders are accountable for up to 80% of crimes, while the remaining 20% of crimes are committed by 80% of offenders. Spelman (1986) analyzed data from four case studies in the United States and England and observed that around 10% of offenders accounted for around 40% of crimes. Other researchers have found even greater levels of concentration. Wolfgang et al. (1972), for example, found that 6% of juveniles from Philadelphia, who represented 18% of all juvenile offenders in the sample of their birth cohort study, accounted for 52% of all contacts with the police. Similarly, Sampson and Laub (2003) found that 7.5% of men older than 31 arrested by the FBI in 1995 in Massachusetts were responsible for 51% of all crimes registered in the areas under study.

Though these researchers laid the groundwork foundations for criminological research on the concentration of crime in offenders, it is today necessary to conduct new research about the offending concentration on the internet. The internet is an extensive space of interaction that has changed and will continue changing social dynamics, including key social domains affecting finance, politics, and people's everyday life, but also opportunities for crime (Yar and Steinmetz, 2019). We have seen steep increases in cyber-dependent crime and cyber-enabled fraud during the last three decades (Kemp et al., 2021; Kirwan, 2018), while traditional, offline crime has decreased in most Western countries since the mid-1980s (Farrell and Brown, 2016). There is thus a need to comprehend how our understanding of criminal behavior can be applied to the study of crime in cyberspace. There is a growing body of research about the characteristics, activities, and organization of cybercrime offenders (Fox and Holt, 2020; Holt et al., 2016; Leukfeldt and Holt, 2019; Payne et al., 2019). However, it is still to be known the extent to which the repeated observation that criminal behavior concentrates in time and place but also in a few targets and offenders (Eck, 2001; Farrell, 2015), applies to the distribution of online crime (Munksgaard et al., 2019; Paquet-Clouston et al., 2018, 2019). This highlights the need to research the concentration of cybercrime in digital spaces of interaction, times, targets, and offenders.

Just like in physical space, cybercrime tends to concentrate in digital spaces defined by a high 'visibility' and 'accessibility' of likely targets, an absence of capable guardians, and a large frequency and variety of activities conducted by users (Newman and Clarke, 2003). Moreover, the way in which certain online platforms are designed to protect users' anonymity may attract offenders who seek to hide their true identities while committing crime. Cryptomarkets, for example, are eBay-like online platforms which use anonymizing software such as Tor, and almost untraceable cryptocurrencies such as Bitcoin, to allow the trading of drugs and weapons and the obscuring of other criminal activity (Aldridge, 2019). Research also indicates that some internet users suffer multiple forms of repeated victimization (Moneva et al., 2022; Reyns et al., 2011). Regarding the cybercrime offending concentration, there is emerging evidence that a large proportion of cybercriminal behavior may concentrate in just a few offenders. For example, Décary-Hétu and Giammoni (2017) observed signs of concentration of buyers' feedback on a small proportion of cryptomarket drug dealers, Moneva et al. (2020) analyzed survey data from a sample of non-university students who identified themselves as repeated online harassment victims and offenders and noted that criminal behavior concentrated in a few respondents, and Munksgaard et al. (2019) noted that a few tobacco traffickers on cryptomarkets concentrate very large market shares. Paquet-Clouston et al. (2018), Paquet-Clouston et al. (2019) and Burruss et al. (2021) also noted signs of offending concentration in online drug markets, ransomware attacks and website defacements, respectively.

In this research we analyze data from a sample of 186,735 reports of Bitcoin-related cybercrime (i.e., blackmail scam, sextortion, ransomware, and others) recorded from the public data repository BitcoinAbuse (2020) to analyze signs of offending concentration in these data. Our data include information about the Bitcoin address to which the ransom or fraudulent payment was requested, and in some cases paid, as well as details of each incident and the victim reporting. Moreover, we link these data with publicly available Blockchain data for every offender Bitcoin address to obtain further information about potential groups of offenders involved in these criminal activities. For the purpose of this research, 'Bitcoin' refers to the most used decentralized virtual currency, which protects users' identity using cryptography, and thus it is known as a 'cryptocurrency'. The Bitcoin payment system has a *peer-to-peer* network of nodes which validates, certifies, and keeps record of all transactions in blocks that are linked together to form a chain - the Blockchain (Nakamoto, 2008). 'Blockchain' is thus a public ledger where transactions carried out are stored and can be accessed. The original contribution of this paper is thus to illuminate the extent of the 'offender concentration' in cybercrimes that involve payments via Bitcoin and to obtain further information about Bitcoin addresses which appear to concentrate very large numbers of crime reports.

This paper is distributed as follows: First, we present a review of the literature about the offending concentration. Second, we discuss the need to develop research about the concentration of cybercrime. Third, we present our hypotheses followed by a discussion of the data and methods. Fourth, we present our results of the concentration of cybercrime in Bitcoin addresses. Finally, we discuss our conclusions, limitations and policy implications.

The concentration of offending

For many decades, criminologists have observed and presented evidence that crime is unequally distributed amongst the members of society: while most people account for zero or very few crimes, a small proportion of offenders are responsible for the majority of crimes. Such a group of very frequent offenders has been called 'chronic offenders' (Wolfgang et al., 1972), 'persistent offenders' (Hagell and Newburn, 1994) or 'pathological offenders' (Vaughn et al., 2011). But regardless of the label being used, there appears to be enough evidence to demonstrate that the 'offending concentration' applies to most forms of crime and geographic contexts. Martinez et al. (2017) conducted an extensive systematic review and meta-analysis of studies on the 'offending concentration' and concluded that "crime is highly concentrated among a minority of offenders" (Martinez et al., 2017: 12).

Several areas of criminological research have dedicated attention to the study of the 'offending concentration' from different theoretical lenses. We review below some of the main findings in each of these areas of research to describe some of the main contributions in the field.

Glueck and Glueck's (1950) research on juvenile delinquency in Boston was one of the first to observe that while the vast majority of boys who live in criminogenic areas do not become involved in crime, a small proportion of them concentrate large numbers of convictions in court. The Gluecks examined which factors of individuals and families could be predictors of juvenile delinquency (e.g., cohesiveness of families, discipline by father, affection by mother). Wolfgang et al. (1972) examined data from a birth cohort in Philadelphia and observed that more than half of all contacts with the police were associated with only 6% of juveniles in the sample. Since then, developmental and life-course criminologists have studied offender trajectories and analyzed which factors influence the spike in crime during adolescence – among 'adolescence-limited offenders' – and the persistence in criminal offending among those that concentrate many crimes over the course of their lives – 'life-course persistent offenders' (Moffitt, 1993, 2018). While *adolescence-limited offenders* become involved in crime due to a 'maturity gap' between the biological and social maturation processes, *life-course persistent offenders* concentrate many crimes throughout their lives due to certain neurodevelopmental deficits and family risk factors which begin in childhood and persist into midlife.

The study of offender trajectories has also allowed researchers to identify that the concentration of certain crime types in offenders may be due to offenders' crime specialization: offenders accumulate many offences of a given type when they specialize in it, instead of showing more versatile offending patterns. While relatively little evidence of specialization has been found among violent and sexual offenders (Klein, 1984), property crime appears to be conducted with more consistent specialization than violent offences (Blumstein et al., 1988; Miethe et al., 2006). Crime specialization may also vary according to age and developmental stages (Piquero et al., 2007; Moffitt, 2018). Those offenders that accumulate many crimes over the course of their lives, however, are known to be non-specialized and may become involved in broad repertoires of offence types (Mazerolle et al., 2000; Moffitt, 2018).

Crime offending concentrates not only in individuals, but also in families. Other research has found that a few households tend to concentrate large proportions of crime offending. Based on the Cambridge Study in Delinquent Development, which followed 411 London males from 397 families since they were 10 to 40 years old, Farrington et al. (1996) found that 6% of families accounted for half of all convictions, and there was generational transmission of offending from parents to children (i.e., three quarters of convicted fathers had at least a convicted child). Similarly, Lauritsen (1993) analyzed data from the US National Youth Survey and observed that juvenile delinquency concentrated in a very small proportion of households sampled. For instance, the 10% most delinquent households accounted for 100% robberies, 94% serious threats, 87% thefts, and 80% assaults and vandalism. The clustering of crime within families has been explained by the presence of certain genetic factors in families, the learning of crime offending during socialization, mating with partners from other offending families (i.e., assortative mating), or biases of the criminal justice system against certain families (Beaver, 2013; Farrington et al., 2001).

All these studies show that there is a rich body of literature about the 'offending concentration' for traditional, offline crime, while there appears to be a gap in research about the level of concentration of cybercrime among cyber offenders.

The concentration of cybercrime

Cybercrime is on the rise, but so is the general awareness around cyber security and research on the human factor of cybercrime. A new wave of researchers are today applying theories of crime and deviance to cybercrime behavior, and developing new theoretical frameworks to explain the risk of cyber-victimization and persons' involvement in cybercrime offending. As such, cybercrime research presents emerging evidence to show that, just like traditional, offline crime, cybercrime may be highly concentrated in a small proportion of victims and targets, cyber places, times, and offenders.

For instance, cybercrime victimization concentrates in users who become 'visible' in a wide variety of online environments and activities (Leukfeldt and Yar, 2016; Marcum et al., 2010) and there are signs of repeated victimization on the internet (Moneva et al., 2022). Cybercrime also appears to concentrate in space, or cyber-space, and time. As an example, 23% of the more than 43,000 websites sampled by Zarras et al. (2014) concentrated 82% of the whole malicious advertisement recorded; Levchenko et al. (2011) observed that only three banks were providing payment services for more than 95% of all spam-advertised goods in their study; and Rhumorbarbe et al. (2018) showed that 70% of all weapon-related listings in cryptomarkets were concentrated in only two markets called AlphaBay and Dream. Williams et al. (2019) also showed that cybercrime without a clear financial component, such as racist social media posts, concentrate in time after terrorist attacks.

This research focuses specifically on the concentration of cybercrime in offenders. There is also emerging evidence that a small proportion of offenders may account for large proportions of cybercrimes. Arango et al. (2020), for example, obtained data from a large sample of Twitter accounts and noted that 65% of all messages with hateful content, either sexist or racist, were produced by only two users sampled. Moneva et al. (2020) show that online harassment behavior concentrates in some offenders who also identify themselves as repeated victims of online harassment. In the context of online cryptomarkets, Christin (2014) observed that a few sellers concentrate large proportions of items advertised, Décary-Hétu and Giammoni (2017) showed evidence of concentration of buyers' feedback on a small percentage of drug dealers, and Munksgaard et al. (2019) argue that a few tobacco traffickers concentrate very large market shares in cryptomarkets. And recent research has also found strong signs of offending concentration among a few website defacement offenders (Burruss et al., 2021; van de Weijer et al., 2021).

Aside from the theoretical mechanisms discussed in the previous section, which were designed to explain the concentration of offending for more traditional crimes, there are several reasons to explain why cybercrimes may be strongly concentrated among a few offenders. First, the characteristics of the internet, which are less determined by physical constraints than offline environments, have the ability to massively increase the reach of well-designed attacks, which can target thousands of users simultaneously over long periods of time through one-to-many interactions (Miró-Llinares and Moneva, 2020), thus allowing highly specialized offenders to accumulate amounts of crimes impossible to reach through one-to-one interactions. The environmental characteristics of the internet may enlarge the number of potential victims of massive attacks targeting widely used services such as social media platforms or email. The internet, however, also creates opportunities for new types of crimes targeting less used and more specialized services, such as cryptomarkets, where the number of victims and thus the concentration of incidents in offenders may be smaller. Second, the chances of cybercriminals being arrested and convicted may be smaller than that of traditional offenders, which may facilitate that specialized criminals concentrate many offences of the same type over long periods of time without being caught. While not much research has been conducted in this area, one may also expect that those offenders that concentrate large volumes of cyber-attacks also accumulate larger financial gains from criminal activity (Holt et al., 2016; Hunton, 2012). Matsueda et al. (1992), for instance, showed that previous experience with crime was associated with more illegal earnings from crime, and Morselli and Tremblay (2004) found that the more crime an offender commits, the higher his or her illegal earnings.

In this research we analyze the concentration of cybercrimes that involve ransom requests or fraudulent transactions through Bitcoin in Bitcoin addresses. In this sense, a distinction needs to be made between Bitcoin 'address', 'wallet' and 'user'. Any person with access to the internet can create a Bitcoin wallet and become a Bitcoin user. Once users have created a Bitcoin wallet, they can generate as many Bitcoin addresses as they wish, which can then be used to make transactions. Just like in traditional banking systems, users can then share their addresses to send or receive bitcoins. In reality, wallets are not used to store bitcoins, but these simply serve to manage the public and private 'keys' that allow users to access Bitcoin addresses and transfer bitcoins. Thus, a single user can create and manage multiple Bitcoin addresses using a single or multiple wallets. Some researchers have attempted to estimate the average number of Bitcoin addresses per user, and have obtained very different estimates that range from an average of 1.5 addresses per user (Fleder et al., 2015) to 11.6 or 11.9 addresses per user (Androulaki et al., 2013; Santamaria Ortega, 2013). The technological specifications of cryptocurrencies are designed partly to hide the identity of each user of each wallet, and it is almost impossible to know exactly the number of wallets managed by a single user (Reid and Harrigan, 2011). The pseudo-anonymity provided by cryptocurrencies is of course very attractive for those who may benefit from hiding their identity. For instance, Europol argues that the "distributed nature [of cryptocurrencies] makes them resistant to law enforcement disruption and government control" (Europol, 2014). This is the reason why cryptocurrencies have become a common payment mechanism in crimes involving extortion (e.g., ransomware, DDoS attacks, or sextortion), online shopping frauds, payments in Darknet markets (e.g., to acquire data, hacking software, illegal drugs or other services), as well as to hide criminal-to-criminal payments associated with illegal activities (Palisse et al., 2017).

Hypotheses

Based on the literature review presented above, we devise the following hypotheses that will be addressed in our research:

H1. A large proportion of Bitcoin-related cybercrime will be associated with a small proportion of Bitcoin addresses.

H2. Cybercrimes which target users of widely used services (e.g., email, social media) are defined by a larger offending concentration than cybercrimes targeting users of less widespread services (e.g., cryptomarkets).

H3. Bitcoin addresses that concentrate a large proportion of cybercrime reports also concentrate more overall transaction activity and financial gain.

Data and methods

This section describes the data and methods used to address our hypotheses. Data for this research have been collected from two different sources: BitcoinAbuse and Blockchain. Firstly, we have gathered a large dataset of victim reports of Bitcoin-related cybercrime from the public data repository BitcoinAbuse (2020). In these reports, Bitcoin transactions are requested, and in some cases paid, as ransom or fraudulent payments. This database is created through a self-reported victimization form by which victims access the BitcoinAbuse website (https://www.bitcoinabuse.com/) and report the Bitcoin address of the offender, the type of crime, information about the abuser, and a detailed description of each crime. The dataset also includes information about the country of residence of victims and the time of each report. We used the website API to download all reports registered from 16 May 2017 to 15 October 2020.[1]

In total, we collected a sample of 186,735 reports which include the following information: a unique identifying number for each report, Bitcoin address where money was requested/sent, type of offence (i.e., ransomware, blackmail scam, sextortion, darknet market fraud, Bitcoin tumbler fraud or other), country of victim (based on IP address), date in which the victim reported the crime, and a free text question that victims can use to provide details of the incident or copy the message received. These data include information from a self-selected, non-probability sample of victims of Bitcoin-related cybercrime which is not necessarily representative of the whole universe of victims. It is likely, for example, that victims from some countries are more familiarized with this platform than others, and tech-savvy victims may be more willing to share some information but not other details. Regardless of the limitations of the non-random mode of production of these data, it is an extremely rich and valuable source of information to gain insights into the concentration of cybercrime and some characteristics of cyber offenders. For instance, while the biases implicit in our data likely create threats to the reliability of information about victims, since it is likely that not all victims of Bitcoin-related attacks have equal probabilities to report, we do not have indicators that the non-probability nature of our sample affect the reliability of information about Bitcoin accounts linked with crime, which will be used in our study. In other words, we do not expect that the chances of an incident being reported vary depending on the characteristics of the Bitcoin address responsible for the incident. As such, this dataset has been used for research with different purposes: Azani et al. (2020) used these data to check if a Bitcoin address had been reported as having links with the Hamas organization,

[1] More information about BictoinAbuse API can be found in https://www.bitcoinabuse.com/api-docs. The API allows downloading the 'csv' file with all reports within a given period (i.e., one day, 30 days, or forever). In order to download the data, it is necessary to obtain an API key first, which can be obtained freely as well.

Oggier et al. (2020) studied the linguistic characteristics of reports related to a particular Bitcoin address, and Xia et al. (2020) analyzed the rise in COVID-19-related scams which include certain keywords.

The BitcoinAbuse dataset records information for the following crime types:

- *Ransomware:* it is a type of malware which blocks or encrypts users' systems, files and computers and demands the payment of a ransom to reinstate access to the system or decrypt files. The ransom payment is demanded in Bitcoin. This category includes reports in which victims have been affected by malware downloaded via email or infected websites which block the users' systems or encrypt their files.
- *Blackmail scam:* victims receive a message, usually via email, which claims that their system has been accessed or hacked, and offenders threaten to release some embarrassing information or personal details unless a certain amount is paid in Bitcoin. Sometimes personal information of the victim is added to give credibility to the threat.
- *Sextortion:* in general, 'sextortion' refers to blackmailing someone to either obtain sexual favors or threaten the victim with publishing sexually explicit information, images or videos unless a certain amount is paid. In our data, most reports under this category refer to threats in which the blackmailer claims to have compromising information about the victims (e.g., videos or images accessed via webcam, information about porn sites visited, or pornographic content found in the victim's computer) and asks for a ransom to prevent such information being published.
- *Darknet market*: these refer to online markets in the Darknet where people can buy illegal goods (mostly drugs, but also firearms, malware software, credit card details, and others) or pay for some illegal service using cryptocurrencies such as Bitcoin and Monero. In our data, reports under this category mainly refer to frauds committed by Darknet market sellers who do not provide the product or service the victim paid for, but also some reports of Darknet markets offering illegal services and Bitcoin accounts with links to illegal products advertised in Darknet markets.
- *Bitcoin tumblers*: Bitcoin tumblers, which are also known as Bitcoin mixers, are services that mix potentially identifiable Bitcoin transactions to obscure the trail of the original source, which otherwise would be publicly available in Blockchain. In our data, reports under this category refer to fraudulent Bitcoin mixing services that steal user's cryptocurrencies.
- *Other*: other Bitcoin-related crimes not classified in the previous categories.

As shown in Table 1, blackmail scam was the most commonly reported crime type, followed by sextortion and ransomware, while the proportion of reports associated with Bitcoin tumbler scams and Darknet markets was much smaller. The decision about which crime category describes better the crime incident being reported is taken by victims, and in some cases there may be classification errors.

Table 1. Crime types recorded in BictoinAbuse data

	Frequency	Percentage
Blackmail scam	75,372	40.4%
Sextortion	59,041	31.6%
Ransomware	42,398	22.7%
Other	7,288	3.9%
Bitcoin tumbler	1,824	1.0%
Darknet market	812	0.4%

We can also see in Table 2 that more than 27% of all crimes were reported by victims from the United States, but victims from the United Kingdom, Canada, Germany and France also represent a large frequency of reports. In total, victims from 218 countries are represented in the data.

Table 2. Top 10 countries represented in BitcoinAbuse data by victims' residence

	Frequency	Percentage
United States	50,872	27.2%
United Kingdom	15,921	8.5%
Canada	11,505	6.2%
Germany	9,173	4.9%
France	8,023	4.3%
Netherlands	6,192	3.3%
Australia	5,079	2.7%
Japan	3,886	2.1%
Sweden	3,701	2.0%
Spain	3,666	2.0%

In order to obtain further information about the characteristics of each Bitcoin address reported, we downloaded data from the public repository Blockchain.com, which records data for cryptocurrency transactions and Bitcoin addresses and makes it public through an API.[2] First, we grouped all cybercrime reports by Bitcoin address and created a dataset of 54,033 addresses reported. Then, we used the Blockchain API to download public data about the overall number of transactions, overall number of bitcoins received and sent, and final balance for every Bitcoin address reported in our data. Additional data for 45,500 addresses was accessed from Blockchain, while 8,533 addresses did not have additional information recorded in Blockchain (these were incorrectly recorded in the report or did not exist). Summary statistics of data about Bitcoin addresses represented in both the BitcoinAbuse and Blockchain datasets (n=45,500) are described in Table 3. Summary statistics in Table 3 already show signs of offending concentration, with the vast majority of addresses concentrating very small values of crime reports, transactions, bitcoins received and sent, final balance, days active, countries with reports, and crime types attempted, and a very small proportion of accounts accumulating very large values in each of these variables. We will further analyze this in the next section. It is important to note, however, that the value of Bitcoin is highly volatile, and it suffered remarkable changes during the period of our study. The value of one Bitcoin varied from 1,750 USD in May 2017 to 11,444 USD in October 2020. Thus, it is likely that some of the addresses that concentrate very large amounts of Bitcoins received or sent are due to bitcoins transferred when their value was much lower. We downloaded data from Blockchain in October 2020, before the value of bitcoin skyrocketed in December 2020 and peaked in April 2021 (1 Bitcoin = 63,224 USD).

[2] More information about the Blockchain API can be found in https://www.blockchain.com/api.

Table 3. Summary statistics of information about Bitcoin addresses reported in BitcoinAbuse

	Min	First quartile	Median	Mean	Third quartile	Max
Number of reports*	1.0	1.0	1.0	3.3	2.0	950.0
Number of transactions**	0.0	0.0	0.0	304.0	0.0	3387485.0
Bitcoin received**	0.0	0.0	0.0	6354.0	0.0	132302782.0
Bitcoin sent**	0.0	0.0	0.0	6337.0	0.0	132302233.0
Balance on Blockchain**	0.0	0.0	0.0	16.6	0.0	141451.6
Days between first and last report*	1.0	1.0	1.0	7.3	1.0	1186.0
Number of countries with reports*	1.0	1.0	1.0	1.8	1.0	85.0
Number of crime types attempted*	1.0	1.0	1.0	1.3	1.0	6.0

*Obtained from BitcoinAbuse; **Obtained from Blockchain

As described above, in this research we analyze the concentration of Bitcoin-related cybercrime reports in Bitcoin addresses, rather than concentration of crime in users or persons. In order to analyze the concentration of crime reports in Bitcoin addresses we will utilize the Lorenz curve and Gini coefficient. The Lorenz curve is a graphical visualization of inequality which was originally developed by Max Lorenz in 1905 to visualize inequality of wealth distribution. The Lorenz curve visualization is generally used to plot which percentage of households, in the *x-axis*, concentrates which percentage of income, in the *y-axis*. For instance, a x-value of 72 and a y-value of 7.5 would represent that the bottom 72% of households account for only 7.5% of the total wealth in a given country, which would be a clear sign of inequality in the distribution, while a line that is closer to the straight $x = y$ line would show that all households have the same amount of wealth. In our case, we will visualize which proportion of Bitcoin addresses concentrate what proportion of Bitcoin-related cybercrime reports. In this sense, a line which is flat at the beginning and rises at the very end would indicate that a few Bitcoin addresses concentrate most crimes, while a straight line that is close to the $x = y$ line would indicate that most accounts account for similar amounts of reports. The ratio of the area between the straight and the curved line is called the Gini coefficient. The Gini coefficient is used to express numerically the extent of inequality in a distribution, and it can range from 0, which shows complete equality, to 1, when one single unit accounts for everything, which could be defined as perfect inequality. For context, according to the World Bank, the Gini index of the United States in 2016 was 0.41, and world values range between 0.25 in Ukraine and 0.63 in South Africa. In the context of the geographic concentration of crime, Bernasco and Steenbeek (2017) analyzed crimes known to the police in The Hague and observed a Gini coefficient of 0.73 for break and enter crimes and 0.86 for assault. We will further expand our analyses with correlation matrices and descriptive statistics. All analyses in this paper have been coded in R software (R Core Team, 2020) with the assistance of the 'ineq' package (Zeileis, 2015). We also computed the 'generalized' version of the Gini index for criminological research developed by Bernasco and Steenbeek (2017), but obtained very similar results to that of the traditional Gini coefficient, and thus we will use the traditional Gini index and Lorenz curve in this paper. All codes and materials are available on a Github repository (https://github.com/davidbuilgil/bitcoin-concentration).

Concentration of cybercrime in Bitcoin addresses

In order to analyze whether a large proportion of Bitcoin-related cybercrime reports are associated with a small proportion of Bitcoin addresses in our data, we first count the number of reports associated with the top 1% accounts with the largest number of reports. In total, 58,063 out of 186,735 reports correspond to only 532 Bitcoin addresses. In other words, 31.1% of crime reports are related to the top 1% of Bitcoin addresses. Similarly, 60.7% reports (i.e., 113,432 out of 186,735 cybercrimes) are related to the top 10% Bitcoin addresses. This is represented more clearly in Figure 1, which shows the Lorenz curve of the concentration of all BitcoinAbuse reports by Bitcoin addresses. As can be seen in Figure 1, the curved dotted line for Bitcoin-related cybercrime is very flat at the beginning, showing, for example, that up to 65% of Bitcoin accounts only account for around 20% of reports, while the curved line rises steeply at the very end, which shows that a few addresses concentrate large proportions of reports. In this case, the Gini coefficient is 0.64, which also shows a large inequality in our distribution. We can thus reject the null hypothesis for H1, as we observe strong signs that Bitcoin-related cybercrime reports are associated with a small proportion of addresses.

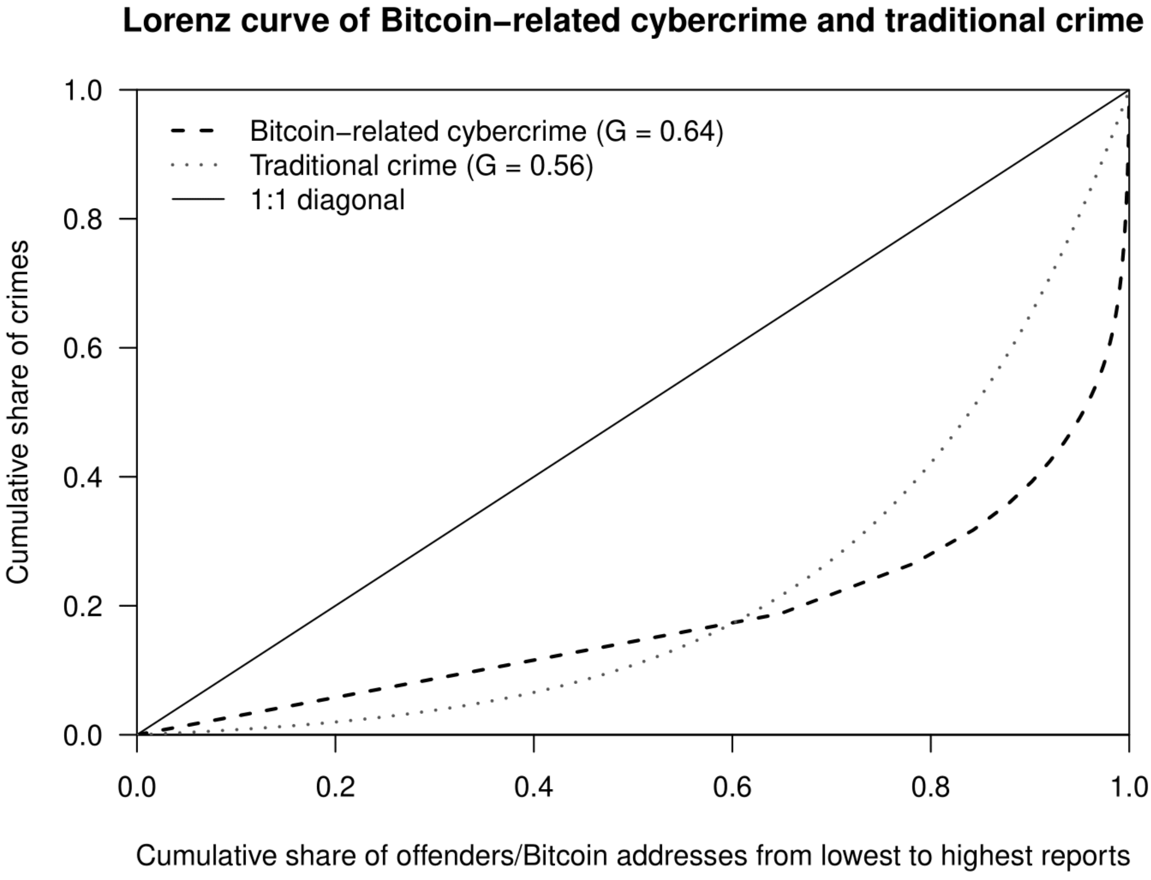


Figure 1. Lorenz curve of concentration of cybercrime and traditional crime in Bitcoin addresses and offenders

Moreover, in order to fully understand the extent of the offending concentration in this distribution, we have compared, also in Figure 1, the Lorenz curve drawn from our data of Bitcoin-related cybercrime with another curve representing traditional offline crime. In order to study the offending concentration for traditional crime, we utilized the regression model parameters computed by Martinez et al. (2017) in their meta-analysis of 27 studies about the frequency of crime offending among criminals. After analyzing the results of these 27 studies, Martinez et al. (2017) calculated that the overall curve of offending concentration follows the model $y = 23.914ln(x) - 13.761$. We used the parameters computed in Martinez et al. (2017) to generate a Lorenz curve of traditional crimes and compare it with the Lorenz curve of Bitcoin-related cybercrime observed in our data. As shown in Figure 1, the distribution of offending appears to be slightly more concentrated in the case of cybercrime than traditional offences. The Gini coefficient for Bitcoin-related cybercrime ($G = 0.64$) is larger than that of traditional crime ($G = 0.56$). While the share of offenders responsible for the first 20% of crimes is very similar in both cases, and the two lines show that around 20% of crimes are only related to around 65% of offenders, the share of crimes concentrated in the most prevalent offenders is remarkably larger in the case of Bitcoin-related cybercrime. For instance, in the case of traditional crime, the 20% most prevalent offenders would concentrate around 60% of crimes, while in our data we observe that the 20% most reported Bitcoin addresses account for around 75% of reports.

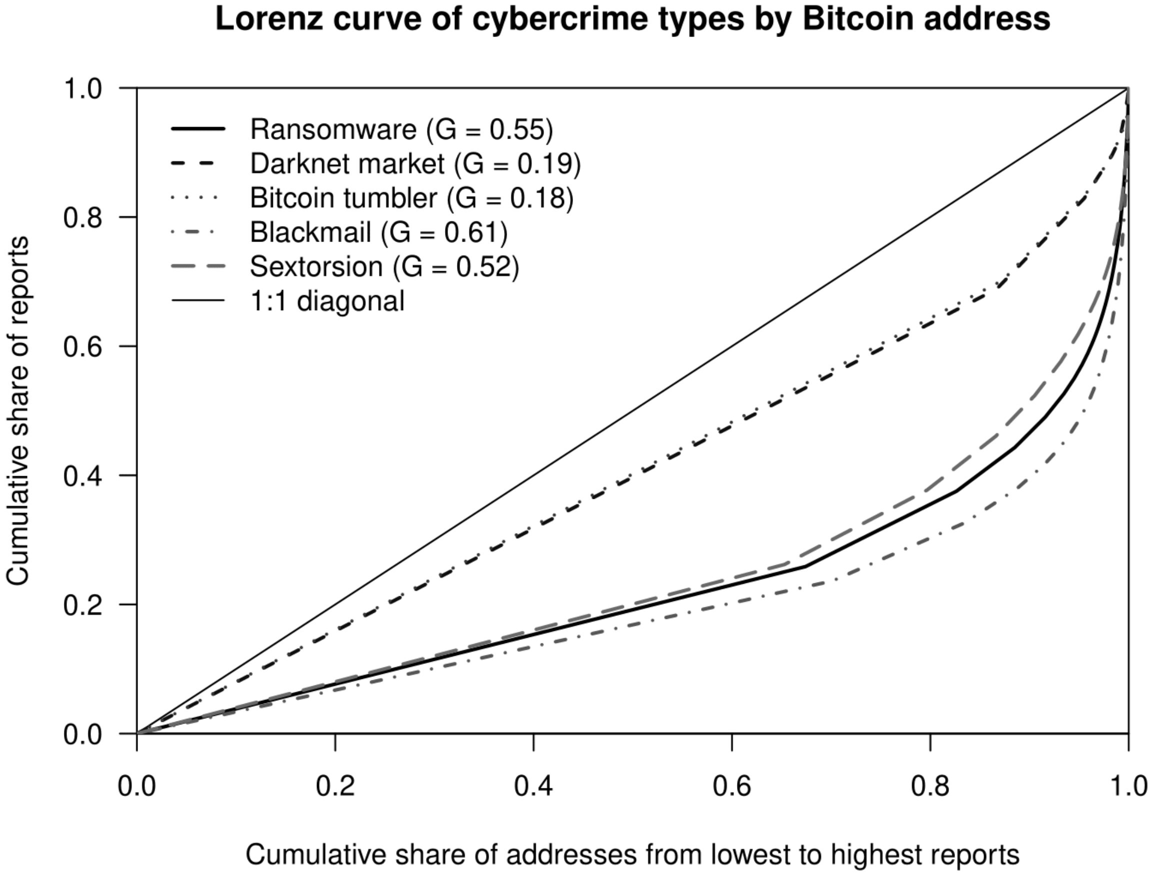


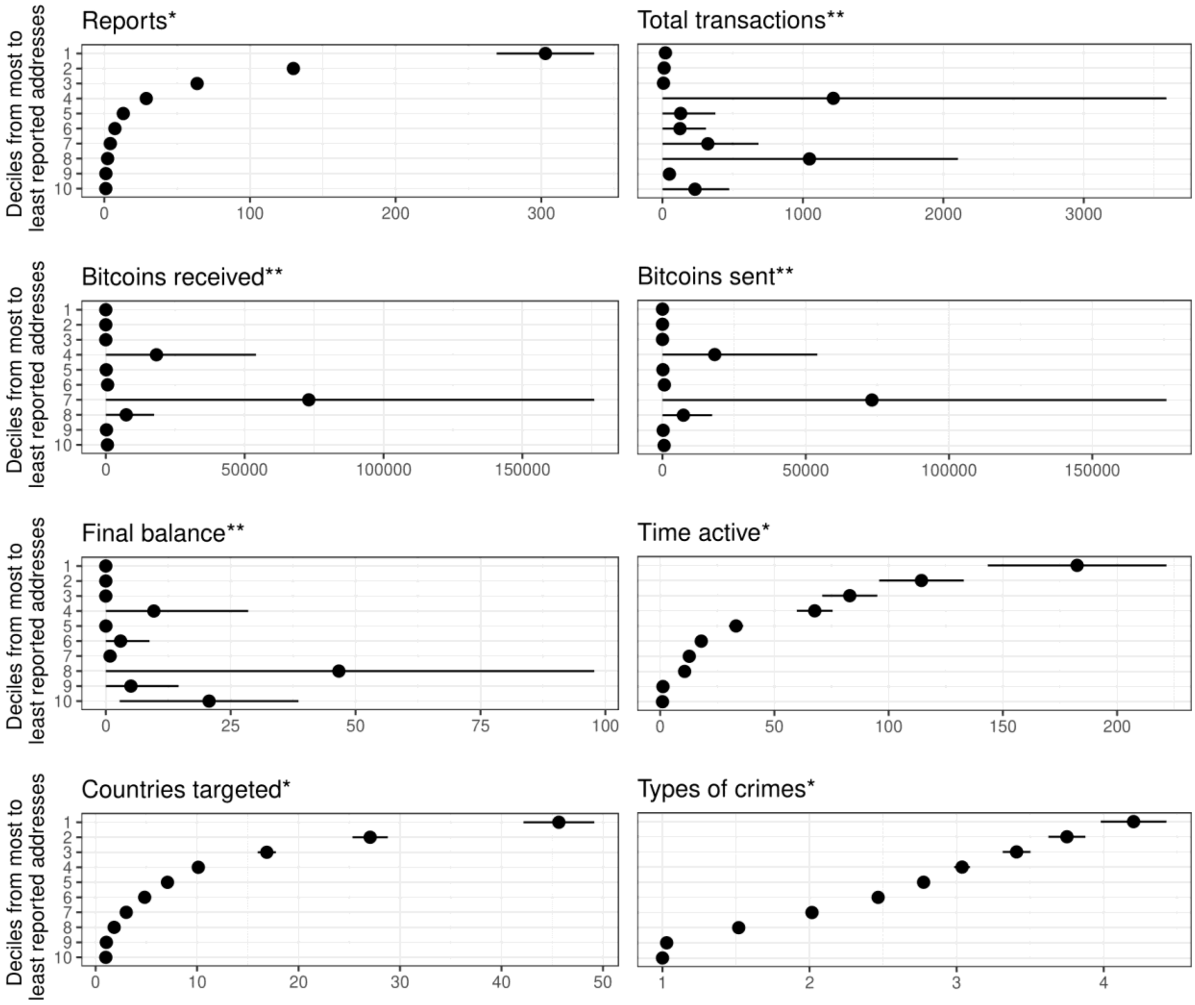
Figure 2. Lorenz curve of concentration of cybercrime types in Bitcoin addresses

Nonetheless, it is likely that not all crime types show the same level of concentration in Bitcoin addresses. We posed in our H2 that those Bitcoin-related cybercrimes which target users of widely used online services, such as email, social media or web browsers, will be defined by a larger offending concentration than cybercrimes targeting users of less widespread services, such as Darknet markets and cryptocurrency mixers, since the former type of attacks can be launched at very large scales and affect many users of digital systems. For example, the same ransomware attack or blackmail scheme may be used to target thousands of users in many countries via email, while fraudulent payments through darknet markets may affect a smaller community of users who buy or sell products through cryptomarkets. Figure 2 shows the Lorenz curves of offending concentration for the five crime types included in our dataset (excluding the category ‘other’), and these indicate that the concentration of reports in Bitcoin addresses is much larger in the case of blackmail scams, ransomware and sextortion, which can target many victims simultaneously, than in the case of frauds through darknet markets and Bitcoin tumblers, which are more likely to target fewer internet users and sometimes be committed through one-to-one interactions. As such, the Gini coefficients for blackmail ($G = 0.61$), ransomware ($G = 0.55$) and sextortion ($G = 0.52$) are much larger than the Gini coefficient for darknet market fraud ($G = 0.19$) and Bitcoin tumbler scam ($G = 0.18$). Thus, we can reject the null hypothesis for H2, since we observe that those crimes which target users of widespread online services can affect many victims simultaneously and are those with the largest Gini coefficients and the most skewed towards the right Lorenz curves.

Concentration of transaction activity in high-crime-density Bitcoin addresses

In order to obtain further information about those Bitcoin addresses that concentrate large quantities of cybercrime reports, and analyze whether these high-crime-density addresses also obtain larger financial benefits in Bitcoin than others, we downloaded Blockchain transaction data for every address represented in our data. Transaction data obtained from Blockchain may represent transactions associated with criminal activities but also legal financial exchanges. We then arranged all Bitcoin addresses represented in both datasets from the address with the largest number of reports to that with the smallest number of reports, and divided our sample of addresses in ten deciles with an equal number of crime reports in each of them. As a result, addresses in the first decile correspond to the most represented addresses that concentrate the top 10% reports, while addresses in the tenth decile are those that received the smallest number of reports and concentrate the bottom 10% of reports. Average values and 95% confidence intervals for each decile are shown in Figure 3.

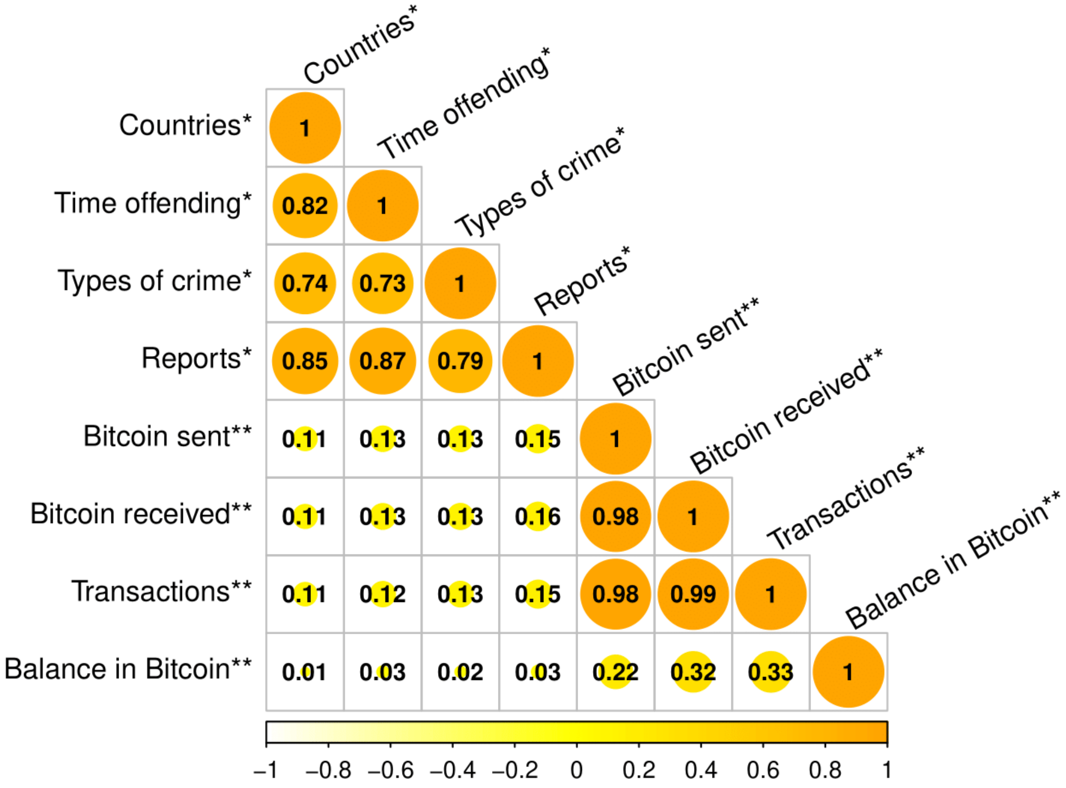
In Figure 3, it can be observed that addresses in the first quartiles (i.e., those that concentrate the largest numbers of reports) are also those that were active during longer periods of time (time between first and last report), targeted more countries and committed more types of crimes (based on categories chosen by victims). However, some surprising patterns can also be observed. First, while addresses in the first quartile show a larger volume of total transactions than addresses in the second and third quartiles, those addresses with the largest average number of Bitcoin transactions, largest average number of bitcoins received and sent, and largest average final balance are not those that received the largest number of crime reports, and they are not located in the second or third decile groups either. Instead, on average, those addresses that received the largest quantities in Bitcoin are located in the seventh, fourth and eighth deciles (i.e., groups located in the central part of the distribution), while those with the largest final balance can be found in the eighth, tenth, fourth and ninth decile groups (i.e., mostly in the lowest part of the distribution). As shown by the 95% confidence intervals, many of those differences are not statistically significant, showing that mean values may be affected by outliers with very large values of total transactions, bitcoins received and sent, and final balance. We also observe that those addresses that receive and send large quantities in Bitcoin are not necessarily those with the largest final balance, independently of the number of cybercrimes attempted.



*Obtained from BitcoinAbuse; **Obtained from Blockchain

Figure 3. Average descriptive information (with 95% confidence intervals) of reported Bitcoin addresses by deciles of concentration of reports

To better illustrate the results presented in Figure 3, we visualize in Figure 4 the Spearman's rank correlation matrix for all variables known. The number of cybercrime reports by Bitcoin address shows very large Spearman's rank correlation coefficients with the number of crime types attempted ($\rho = 0.79, p - value < 0.001$), number of countries targeted ($\rho = 0.85, p - value < 0.001$), and time active between the first and last report ($\rho = 0.87, p - value < 0.001$). Nonetheless, the number of crime reports shows small coefficients of correlation with the amount of Bitcoin received ($\rho = 0.16, p - value < 0.001$) and sent ($\rho = 0.15, p - value < 0.001$) and the number of transactions ($\rho = 0.15, p - value < 0.001$), and a very small correlation coefficient with the final balance ($\rho = 0.03, p - value < 0.001$). In Figure 3, we can also see that the Spearman's rank correlation coefficients between the final balance in Bitcoin and the number of transactions ($\rho = 0.33, p - value < 0.001$), total bitcoins received ($\rho = 0.32, p - value < 0.001$), and total bitcoins sent ($\rho = 0.22, p - value < 0.001$) are all small, while the correlation coefficients between bitcoins received, bitcoins sent, and number of transactions are very large in all cases. Since the correlation between the number of crime reports per Bitcoin address and the financial gain and transaction activity is very weak, we can state that the null hypothesis for H3 is plausible and thus cannot be rejected. Bitcoin addresses that concentrate the largest numbers of cybercrime reports do not appear to be those with more transaction activity and financial gain. Instead, the financial gain and number of transactions of those addresses with very large numbers of cybercrime reports is very small compared to the volume of transactions and bitcoins received by some addresses with smaller concentrations of crime reports.



	Countries*	Time offending*	Types of crime*	Reports*	Bitcoin sent**	Bitcoin received**	Transactions**	Balance in Bitcoin**
Countries*	1							
Time offending*	0.82	1						
Types of crime*	0.74	0.73	1					
Reports*	0.85	0.87	0.79	1				
Bitcoin sent**	0.11	0.13	0.13	0.15	1			
Bitcoin received**	0.11	0.13	0.13	0.16	0.98	1		
Transactions**	0.11	0.12	0.13	0.15	0.98	0.99	1	
Balance in Bitcoin**	0.01	0.03	0.02	0.03	0.22	0.32	0.33	1

*Obtained from BitcoinAbuse; **Obtained from Blockchain

Figure 4. Spearman's rank correlation matrix of measures of cybercrime and transaction activity by Bitcoin account

Discussion and conclusions

Crime research has repeatedly shown that large proportions of crime and deviant behavior tend to concentrate in a few places, times, targets, and offenders. While much research has been dedicated to the study of the concentration of crime for traditional crime, there is a need to expand research about the concentration of cybercrime in digital spaces of interaction (e.g., Rhumorbarbe et al., 2018; Zarras et al., 2014), times of the day and days (e.g., Kemp et al., 2021; Williams et al., 2019), victims and targets (e.g., Holt et al., 2020; Leukfeldt and Yar, 2016), and offenders (e.g., Burruss et al., 2021; Décary-Hétu and Giammoni, 2017; van de Weijer et al., 2021). In this research we accessed a large dataset of 186,735 reports of cybercrimes involving ransom requests and fraudulent payments through Bitcoin (i.e., ransomware, blackmail scam, sextortion, darknet market fraud, and Bitcoin tumbler fraud), and analyzed the concentration of crimes in Bitcoin addresses. Victims of cybercrime used an online platform called BitcoinAbuse to report crime incidents and provide information about the Bitcoin addresses to which the ransom or fraudulent payments were requested or transferred. These data were used to analyze the concentration of Bitcoin-related cybercrime in Bitcoin addresses.

As in traditional crime, a very large proportion of crime reports was associated with just a few addresses that concentrate very large quantities of offences. For instance, the address with the largest frequency of reports concentrated 950 crimes, and the top 1% of addresses accumulated 31.1% of all crimes. The Lorenz curve and Gini coefficient provide strong evidence that large quantities of Bitcoin-related cybercrimes are strongly concentrated in a few Bitcoin addresses. Moreover, in order to explore whether cybercrime reports in our data suffer from a larger or smaller level of crime concentration in offenders than traditional crime, we compared the 'offending concentration' distribution obtained from Martinez et al.'s (2017) meta-analysis of studies about the concentration of traditional offline crimes in offenders with the concentration distribution in our data. Results show that cybercrime is likely to be even more concentrated in offenders than traditional crime. As an example, it is difficult to imagine a single offender accumulating 950 reports of traditional crime over the course of three years and a half, while a single ransomware attack on the internet can accumulate large quantities of victims over very short periods of time. In other words, the internet has the ability to massively increase the reach of crime, and a few offenders may concentrate very large proportions of crimes. It is not only the environmental characteristics of the internet that may contribute to a larger concentration of cybercrime in offenders, but also the level of complexity of the crime types analyzed. Bitcoin-related cybercrimes, unlike more traditional crime types such as violence and sexual offences (Klein, 1984; Miethe et al., 2006), require a level of expertise that may enable tech-savvy offenders to be involved in attacks over long periods of time without being caught, thus becoming specialized in such crimes and concentrating many more attacks than offenders with less refined skills (Leukfeldt and Holt, 2022).

Nonetheless, the level of concentration of cybercrime reports in Bitcoin addresses is not equal for all crime types. For instance, our results show that cybercrimes which target users of widely used services such as email, web browsers, and social media (i.e., ransomware, blackmail, sextortion) show a much larger concentration in Bitcoin addresses than cybercrimes which affect users of less widespread services (i.e., Darknet markets, Bitcoin tumblers). This is because the former, if well designed, can be launched at massive scales and victimize many users simultaneously across many countries in short periods of time, while the latter are much more likely to be committed through one-to-one interactions with users of these less widespread services. Regardless of the level of expertise required in each crime (e.g., ransomware attacks may require more technical expertise than blackmailing someone via email), crimes targeting the wide audience of users of basic internet services accumulate more offending concentration than more targeted offences. Our results also appear to indicate that Bitcoin accounts that concentrate many reports are involved in multiple types of criminal activities on the internet, thus showing certain degree of versatility across offences that require similar skills. Researchers who study the concentration of crime in offenders argue that those offenders who concentrate large values of offending over the course of their lives tend to be non-specialized and are involved in a broad repertoire of crime types especially while they are young (Mazerolle et al., 2000; Moffitt, 2018).

Although cybercrime is likely to be a very profitable criminal endeavor, results presented above show that those Bitcoin addresses that concentrate the largest numbers of reports are not necessarily those that have the largest financial benefits from these activities nor transaction activity in their accounts. Instead, after linking our data of reports of Bitcoin-related cybercrime with publicly available Blockchain data for each Bitcoin address reported in our data, we noted that those addresses that concentrate the largest numbers of transactions and the largest values of Bitcoin received and sent may be those in the central part of the distribution (i.e., those that have been reported, on average, between two and twenty-nine times), whereas addresses with the largest final balance may be, on average, those that concentrate the smallest number of reports (i.e., reported between one and two times). While some of the differences observed across deciles of accounts are driven by the effect of some accounts with very large values (outliers) and are not statistically significant, we have nonetheless observed that those accounts with the largest values in transactions and final balance are not amongst the most frequently reported by victims. There are various explanations that can be posed to explain this, but future research using mixed methods approaches and document analysis of criminal investigations (e.g., Leukfeldt and Holt, 2019; Payne et al., 2019) are needed to illuminate whether these are in fact true. First, it is likely that those Bitcoin addresses that are reported many times are mainly involved in non-sophisticated, non-targeted massive attacks, and persons receiving obviously fake blackmail messages report the attempted attack via BitcoinAbuse but do not pay the ransom requested, while more elaborated, targeted and personalized attacks are perhaps more likely to receive the payment from victims. Second, it is also probable that Bitcoin addresses that concentrate large quantities in Bitcoin transactions diversify their criminal and non-criminal activities, and their financial benefits are not only associated with blackmail and fraud but also with other criminal behavior in cryptomarkets and even links with organized crime and money laundering. Third, while accounts that concentrate large volumes of transactions are likely to be directly or loosely connected with criminal organizations and do not operate independently, given that most of the bitcoins received are later moved onto other accounts and the final balance in these accounts tends to be very small, those accounts with very few reports that have a larger final balances may be associated with individuals operating independently who keep their capital in Bitcoin for their personal financial gain.

Although results presented in this paper are first-of-its-kind and contribute to the understanding of the ‘offending concentration’ for Bitcoin-related cybercrime, this research is not free of limitations. First, we have analyzed the concentration of crime reports in Bitcoin addresses, instead of crimes committed by persons. This is because the technical specifications of Bitcoin are partly designed to prevent disclosing the identity of users managing Bitcoin addresses. Although this may be problematic if the purpose of analyzing these data is to identify individuals who are very active in crime, in truth we expect the concentration of cybercrime in offenders to become even larger to that observed in Bitcoin addresses, with very active offenders managing multiple addresses from which they launch massive attacks and less active offenders managing fewer Bitcoin addresses or only one. Second, data analyzed here is recorded from a non-probability self-selected sample of victims of cybercrime who report their victimization using an online crowdsourcing platform. Literature on the mode of production of crowdsourcing stresses that non-probability samples may be affected by sources of bias that can affect the reliability of outputs obtained from them (Solymosi and Bowers, 2018). While the non-random nature of the sample of reports used in this study may present threats to the reliability of information about victims, since some victims may be more likely to report than others, we do not anticipate that the likelihood of crime reporting is affected by the characteristics of the anonymous offenders involved and their Bitcoin addresses. But further research is needed to better understand how data about offenders in our dataset may be affected by potential sources of bias. And third, the value of Bitcoin suffered important changes during the period of our study, and some accounts could concentrate very large amounts of bitcoins received and sent when the value of this cryptocurrency was much lower.

Results presented in this paper may also serve to guide policing operational decisions and policy making to prevent Bitcoin-related cybercrime. For instance, we have shown that those Bitcoin addresses that concentrate very large quantities of crime reports are not necessarily those that gain the largest quantities from being involved in criminal activities, and thus police investigations may prioritize investigating those addresses with very large benefits instead of those that concentrate many reports. Moreover, combining data about cybercrime reports with public Blockchain data allows gaining information about Bitcoin addresses that may be part of larger criminal organizations involved in multiple forms of criminal offending. Developing an understanding of the dynamics and 'scripts' of cybercrimes which involve the use of Bitcoin transactions may also serve to design awareness campaigns for victims to know how to prevent these attacks and how to react once a blackmail email is received or a ransomware attack infects one's system. Results presented in this article also help illuminate the extent to which cyber offenders specialize in certain crime types, which may have important implications for policy and practice (Leukfeldt and Holt, 2022). While we have not analyzed if offenders who commit cybercrime are also involved in other types of incidents offline, it is likely that our results are partly driven by a high degree of specialization of cyber offenders, who can repeatedly victimize hundreds of users through one-to-many interactions with little risk of detection. Public administrations and police forces may enhance actions to increase the perceived risk of detection of those cybercrimes that are conducted with more consistent specialization, which should in turn contribute to reducing the number of attacks launched by specialized offenders. Nonetheless, there is a need for new research on Bitcoin-related cybercrime. Future research may analyze and categorize clusters of Bitcoin addresses involved in crime, and utilize Blockchain data and social network analysis to track the movement of bitcoins obtained from criminal activity across Bitcoin addresses.

References

Aldridge, Judith. 2019. “Does online anonymity boost illegal market trading?” *Media, Culture & Society* 41(4):578-583. doi:10.1177/0163443719842075

Androulaki, Elli, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. “Evaluating user privacy in Bitcoin.” Pp. 34-51 in *Financial cryptography and data security*, edited by Ahmad-Reza Sadeghi. Berlin: Springer. doi:10.1007/978-3-642-39884-1_4

Arango, Aymé, Jorge Pérez, and Barbara Poblete. 2019. “Hate speech detection is not as easy as you may think: A closer look at model validation”. Pp 45-54 in *Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR'19)*. Association for Computing Machinery. doi:10.1145/3331184.3331262

Azani, Eitan, Michael Barak, Edan Landau, and Nadine Liv. 2020. *Identifying money transfers and terror finance infrastructure in the service of the popular resistance committees in Gaza*. COBWEBS. Retrieved from: https://www.ict.org.il/Article/2488/Identifying_Money_Transfers_and_Terror_Finance_Infrastructure#gsc.tab=0

Beaver, Kevin M. 2013. “The familial concentration and transmission of crime.” *Criminal Justice and Behavior* 40(2):139-155. doi:10.1177/0093854812449405

Bernasco, Wim, and Wouter Steenbeek. 2017. “More places than crimes: Implications for evaluating the law of crime concentration at place.” *Journal of Quantitative Criminology* 33:451-467. doi:10.1007/s10940-016-9324-7

BitcoinAbuse. 2020. *Bitcoin Abuse Database*. Retrieved from: https://www.bitcoinabuse.com/

Blumstein, Alfred, Jacqueline Cohen, Somnath Das, and Soumyo D. Moitra. 1988. “Specialization and seriousness during adult criminal careers.” *Journal of Quantitative Criminology* 4(4):303-345.

Burruss, George W., C. Jordan Howell, David Maimon, and Fangzhou Wang. 2021. “Website defacer classification: A finite mixture model approach.” *Social Science Computer Review*. doi:10.1177/0894439321994232

Christin, Nicolas. 2013. “Traveling the silk road: A measurement analysis of a large anonymous online marketplace.” Pp 213-224 in *Proceedings of the 22nd international conference on World Wide Web*. Association for Computing Machinery. doi:10.1145/2488388.2488408

Clarke, Ronald V., and John E. Eck. 2005. *Crime analysis for problem solvers in 60 small steps.* Washington DC: Center for Problem Oriented Policing. Retrieved from: https://cops.usdoj.gov/RIC/Publications/cops-p080-pub.pdf

Décary-Hétu, David, and Luca Giommoni. 2017. “Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous.” *Crime, Law and Social Change* 67(1):55-75. doi:10.1007/s10611-016-9644-4

Eck, John E. 2001. “Policing and crime event concentration.” Pp 249-276 in *The process and structure of crime: Criminal events and crime analysis*, edited by Robert F. Meier, Leslie W. Kennedy and Vincent F. Sacco. New Brunswick: Transaction Publishers.

Europol. 2014. *Internet organised crime threat assessment (iOCTA) 2014*. Retrieved from: https://www.europol.europa.eu/iocta/2014/chap-3-5-view1.html

Farrell, Graham. 2015. “Crime concentration theory.” *Crime Prevention and Community Safety* 17:233-248. doi:10.1057/cpcs.2015.17

Farrell, Graham, and Rick Brown. 2016. “On the origins of the crime drop: Vehicle crime and security in the 1980s.” *The Howard Journal of Crime and Justice* 55:226-237. doi:10.1111/hojo.12158

Farrington, David P., Geoffrey C. Barnes, and Sandra Lambert. 1996. “The concentration of offending in families.” *Legal and Criminological Psychology* 1(1):47-63. doi:10.1111/j.2044-8333.1996.tb00306.x

Farrington, David P., Darrick Jolliffe, Rolf Loeber, Magda Stouthamer-Loeber, and Larry M. Kalb. 2001. “The concentration of offenders in families, and family criminality in the prediction of boys' delinquency.” *Journal of Adolescence* 24(5):579-596. doi:10.1006/jado.2001.0424

Fleder, Michael, Michael S. Kester, and Sudeep Pillai. 2015. “Bitcoin transaction graph analysis.” *arXiv*. Retrieved from: https://arxiv.org/abs/1502.01657

Fox, Bryanna, and Thomas J. Holt. 2020. “Use of a multitheoretic model to understand and classify juvenile computer hacking behavior.” *Criminal Justice and Behavior*. doi:10.1177/0093854820969754

Glueck, Sheldon, and Eleanor Glueck. 1950. *Unraveling juvenile delinquency.* New York: The Commonwealth Fund.

Hagell, Ann, and Tim Newburn, T. 1994. *Persistent young offenders*. London: Policy Studies Institute.

Holt, Thomas J., Rutger Leukfeldt, and Steve van de Weijer. 2020. “An examination of motivation and routine activity theory to account for cyberattacks against Dutch web sites.” *Criminal Justice and Behavior*. doi:10.1177/0093854819900322

Holt, Thomas J., Olga Smirnova, and Yi Ting Chua. 2016. “Exploring and estimating the revenues and profits of participants in stolen data markets.” *Deviant Behavior* 37(4):353-367. doi:10.1080/01639625.2015.1026766

Hunton, Paul. 2012. “Data attack of the cybercriminal: Investigating the digital currency of cybercrime.” *Computer Law & Security Review* 28(2):201-207. doi:10.1016/j.clsr.2012.01.007

Kemp, Steven, David Buil-Gil, Asier Moneva, Fernando Miró-Llinares, and Nacho Díaz-Castaño. 2021. “Empty streets, busy Internet. A time series analysis of cybercrime and fraud trends during COVID-19.” *Journal of Contemporary Criminal Justice* OnlineFirst. doi:10.1177/10439862211027986

Kirwan, Grainne H. 2018. “The rise of cybercrime.” In *The Oxford Handbook of Cyberpsychology*, edited by Alison Attrill-Smith, Chris Fullwood, Melanie Keep and Daria J. Kuss. Oxford University Press. doi:10.1093/oxfordhb/9780198812746.013.32

Klein, Malcolm W. 1984. “Offence specialisation and versatility among juveniles.” *British Journal of Criminology* 24(2):185-194. doi:10.1093/oxfordjournals.bjc.a047439

Lauritsen, Janet L. 1993. “Sibling resemblance in juvenile delinquency: Findings from the National Youth Survey.” *Criminology* 31(3):387-409. doi:10.1111/j.1745-9125.1993.tb01135.x

Leukfeldt, E. Rutger, and Thomas J. Holt. 2019. “Examining the social organization practices of cybercriminals in the Netherlands online and offline.” *International Journal of Offender Therapy and Comparative Criminology* 64(5):522-538. doi:10.1177/0306624X19895886

Leukfeldt, Eric Rutger, and Thomas J. Holt. 2022. “Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals.” *Computers in Human Behavior* 126:106979. doi:10.1016/j.chb.2021.106979

Leukfeldt, Eric Rutger, and Majid Yar. 2016. “Applying routine activity theory to cybercrime: A theoretical and empirical analysis.” *Deviant Behavior* 37(3):263-280. doi:10.1080/01639625.2015.1012409

Levchenko, Kirill, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Mark Felegyhazi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage. 2011. “Click trajectories: End-to-end analysis of the spam value chain.” Pp 431-446 in *2011 IEEE Symposium on Security and Privacy*. IEEE. doi:10.1109/SP.2011.24

Marcum, Catherine D., George E. Higgins, and Melissa L. Ricketts. 2010. “Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory.” *Deviant Behavior* 31(5):381-410. doi:10.1080/01639620903004903

Martinez, Natalie N., YongJei Lee, John E. Eck, and SooHyun O. 2017. “Ravenous wolves revisited: a systematic review of offending concentration.” *Crime Science* 6(10). doi:10.1186/s40163-017-0072-2

Matsueda, Ross L., Rosemary Gartner, Irving Piliavin, and Michael Polakowski. 1992. “The prestige of criminal and conventional occupations: A subcultural model of criminal activity.” *American Sociological Review* 57:752-770. doi:10.2307/2096121

Mazerolle, Paul, Robert Brame, Ray Paternoster, Alex Piquero, and Charles Dean. 2000. “Onset age, persistence, and offending versatility: Comparisons across gender.” *Criminology* 38(4):1143-1172. doi:10.1111/j.1745-9125.2000.tb01417.x

Miethe, Terence D., Jodi Olson, and Ojmarrh Mitchell. 2006. “Specialization and persistence in the arrest histories of sex offenders: A comparative analysis of alternative measures and offense types.” *Journal of Research in Crime and Delinquency* 43(3):204-229. doi:10.1177/0022427806286564

Miró-Llinares, Fernando, and Asier Moneva. 2020. “Environmental criminology and cybercrime: Shifting the focus from the wine to the bottles.” Pp. 491-511 in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, edited by Thomas J. Holt and Adam M. Bossler. Springer. doi:10.1007/978-3-319-78440-3_30

Moffitt, Terrie E. 1993. “Adolescence-limited and life-course-persistent antisocial behavior: A developmental taxonomy.” *Psychological Review* 100(4):674-701. doi:10.1037/0033-295X.100.4.674

Moffitt, Terrie E. 2018. “Male antisocial behaviour in adolescence and beyond.” *Nature Human Behavior* 2:177-186. doi:10.1038/s41562-018-0309-4

Moneva, Asier, Fernando Miró-Llinares, and Timothy C. Hart. 2020. “Hunter or prey? Exploring the situational profiles that define repeated online harassment victims and offenders.” *Deviant Behavior.* doi:10.1080/01639625.2020.1746135

Moneva, Asier, E. Rutger Leukfeldt, Steve G. A. Van De Weijer, and Fernando Miró-Llinares. 2022. “Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective.” *Computers in Human Behavior* 126:106984. doi:10.1016/j.chb.2021.106984

Morselli, Carlo, and Pierre Tremblay. 2004. “Criminal achievement, offender networks and the benefits of low self-control.” *Criminology* 42(3):773-804. doi:10.1111/j.1745-9125.2004.tb00536.x

Munksgaard, Rasmus, David Décary-Hétu, Vincent Mousseau, and Aili Malm. 2019. "Diversification of tobacco traffickers on cryptomarkets." *Trends in Organized Crime.* doi:10.1007/s12117-019-09375-6

Nakamoto, Satoshi. 2008. *Bitcoin: A peer-to-peer electronic cash system*. Bitcoin. Retrieved from: https://bitcoin.org/bitcoin.pdf

Newman, Graeme R., and Ronald V. Clarke. 2003. *Superhighway robbery: Preventing e-commerce crime*. Portland: Willan Publishing

Oggier, Frédérique, Anwitaman Datta, and Silivanxay Phetsouvanh. 2020. "An ego network analysis of sextortionists." *Social Network Analysis and Mining* 10(1):44. doi:10.1007/s13278-020-00650-x

Paquet-Clouston, Masarah, David Décary-Hétu, and Carlo Morselli. 2018. "Assessing market competition and vendors' size and scope on AlphaBay." *International Journal of Drug Policy* 54:87-98. doi:10.1016/j.drugpo.2018.01.003

Paquet-Clouston, Masarah, Bernhard Haslhofer, and Benoit Dupont. 2019. "Ransomware payments in the Bitcoin ecosystem." *Journal of Cybersecurity* 2019:1-11. doi:10.1093/cybsec/tyz003

Palisse, Aurélien, Hélène Le Bouder, Jean Louis Lanet, Colas Le Guernic, and Axel Legay. 2017. "Ransomware and the Legacy Crypto API." Pp. 11-28 in *Risks and Security of Internet and Systems*, edited by Frédéric Cuppens, Nora Cuppens, Jean-Louis Lanet and Axel Legay. Springer. doi:10.1007/978-3-319-54876-0_2

Payne, Brian, David C. May, D, and Lora Hadzhidimova. 2019. "America's most wanted criminals: comparing cybercriminals and traditional criminals." *Criminal Justice Studies* 32(1). doi:10.1080/1478601X.2018.1532420

Piquero, Alex R., David P. Farrington, and Alfred Blumstein. 2007. *Key issues in criminal career research: New analyses from the Cambridge Study in Delinquent Development*. New York: Cambridge University Press.

R Core Team. 2020. *R: A language and environment for statistical computing.* R Foundation for Statistical Computing, Vienna, Austria. Retrieved from: https://www.R-project.org/

Reid, Fergal, and Martin Harrigan. 2011. "An analysis of anonymity in the Bitcoin system." Pp. 1318-1326 in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*. IEEE. doi:10.1109/PASSAT/SocialCom.2011.79

Reyns, Bradford W., Billy Henson, and Bonnie S. Fisher. 2011. "Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization." *Criminal Justice and Behavior* 38(11):1149-1169. doi:10.1177/0093854811421448

Rhumorbarbe, Damien, Denis Werner, Quentin Gilliéron, Ludovic Staehli, Julian Broséus, and Quentin Rossy. 2018. "Characterising the online weapons trafficking on cryptomarkets." *Forensic Science International* 283:16-20. doi:10.1016/j.forsciint.2017.12.008

Sampson, Robert J., and John H. Laub. 2003. "Life-course desisters? Trajectories of crime among delinquent boys followed to age 70." *Criminology* 41(3):301-340. doi:10.1111/j.1745-9125.2003.tb00997.x

Santamaria Ortega, Marc. 2013. *The Bitcoin transaction graph anonimity*. MSc thesis, Autonomous University of Barcelona. Retrieved from:

http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23562/9/msantamariaoTFM0613memoria.pdf

Solymosi, Reka, and Kate Bowers. 2018. The role of innovative data collection methods in advancing criminological understanding. Pp. 210-237 in *The Oxford handbook of environmental criminology*, edited by Gerben J. N. Bruinsma and Shane D. Johnson. Oxford University Press. doi:10.1093/oxfordhb/9780190279707.013.35

Spelman, William. 1986. *The depth of a dangerous temptation: Another look at selective incapacitation*. Washington DC: US National Institute of Justice.

van de Weijer, Steve G. A., Thomas J. Holt, and E. Rutger Leukfeldt. 2021. “Heterogeneity in trajectories of cybercriminals: A longitudinal analyses of web defacements.” *Computers in Human Behavior Reports* 4. doi:10.1016/j.chbr.2021.100113

Vaughn, Michael G., Matt DeLisi, Tracy Gunter, Qiang Fu, Kevin M. Beaver, Brian E. Perron, Matthew O. Howard. 2011. “The severe 5%: A latent class analysis of the externalizing behavior spectrum in the United States.” *Journal of Criminal Justice* 39(1):75-80. doi:10.1016/j.jcrimjus.2010.12.001

Williams, Matthew L., Pete Burnap, Amir Javed, Han Liu, and Sefa Ozalp. 2020. “Hate in the machine: Anti-black and Anti-muslim social media posts as predictors of offline racially and religiously aggravated crime.” *British Journal of Criminology* 60(1):93-117. doi:10.1093/bjc/azz049

Wolfgang, Marvin E., Robert M. Figlio, and Thorsten Sellin. 1972. *Delinquency in a birth cohort*. Chicago: University of Chicago Press.

Xia, Pengcheng, Haoyu Wang, Xiapu Luo, Lei Wu, Yajin Zhou, Guangdong Bai, Guoai Xu, Gang Huang, and Xuanzhe Liu. 2020. “Don’t fish in troubled waters! Characterizing coronavirus-themed cryptocurrency scams.” *ArXiv*. Retrieved from: http://arxiv.org/abs/2007.13639

Yar, Majid, and Kevin F. Steinmetz. 2019. *Cybercrime and society*. Third edition. London: SAGE.

Zarras, Apostolis, Alexandros Kapravelos, Gianluca Stringhini, Thorsten Holz, Christopher Kruegel, and Giovanni Vigna. 2014. “The dark alleys of Madison Avenue: Understanding malicious advertisements.” Pp 373-380 in *IMC '14: Proceedings of the 2014 Conference on Internet Measurement Conference*. Association for Computing Machinery. doi:10.1145/2663716.2663719

Zeileis, Achim. 2015. *ineq: Measuring inequality, concentration, and poverty*. R package version 0.2-13. Retrieved from: https://cran.r-project.org/web/packages/ineq/index.html