Cyber 9/11 Will Not Take Place: A User Perspective of Bitcoin and Cryptocurrencies from Underground and Dark Net Forums

Simon Butler* [0000-0001-9547-1558]

Information Security Group, Royal Holloway, University of London, UK
Simon.Butler.2015@live.rhul.ac.uk

Abstract. Background. There is a historical narrative of fear surrounding cybercrime. This has extended to cryptocurrencies (CCs), which are often viewed as a criminal tool. **Aim.** To carry out the first user study of CCs for illicit activity, from the perspective of underground and dark net forums. **Method.** We conducted a qualitative study, using a content analysis method, of 16,405 underground and dark net forum posts selected from *CrimeBB*, a dataset of 100 million posts curated by the Cambridge Cybercrime Centre. **Results.** Firstly, finality of payments emerged as a major motivator for the use of CCs. Second, we propose an Operational Security Taxonomy for Illicit Internet Activity to show that CCs are only one part of several considerations that combine to form security in illicit internet transactions. Third, the dark net is hard to use and requires significant study, specialist equipment and advanced knowledge to achieve relative security. **Conclusion.** We argue that finality is the main advantage of CCs for this user group, not anonymity as widely thought. The taxonomy shows that banning CCs is unlikely to be effective. Finally, we contend that the dark net is a niche for criminal activity and fears over cybercrime cause the threat to be exaggerated.

Keywords: Bitcoin, Cryptocurrencies, Underground and Dark Net Forums, User Studies, Cybercrime, Security.

1 Introduction

On the 25 February 2015, the Superintendent of New York State's Department of Financial Services (DFS) delivered a speech at Columbia Law School about the role of regulators after the Great Financial Crisis. In a section on cyber security in the financial sector, the Superintendent made clear the extent of his department's fears:

> We are concerned that within the next decade (or perhaps sooner) we will experience an Armageddon-type cyber event that causes a significant disruption in the financial system for a period of time – what some have termed a "cyber 9/11". [1]

* Simon Butler was supported as part of the EPSRC Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/K035584/1).

On the very same day, DFS released its revised proposed rules for businesses with CC services; the so-called 'Bitlicense' regulation, which came into force a few months later. This highlights the rhetoric of extreme fear that often surrounds matters of cybercrime. Indeed, for several decades there were predictions that 'Cyberwar is Coming!', to which Thomas Rid responded that 'Cyber War Will Not Take Place' [2].

The narrative surrounding CCs has also often been security led, providing ample material for the media. Stories have run of the FBI's fears of Bitcoin's popularity with criminals [3], of the Chairman of the Federal Reserve commenting that CCs are 'great if you are trying to hide or launder money' [4] or even more recently, in 2019, when CCs made headlines when described as a national security threat by the US Treasury Secretary [5]. There is a War on Terror, a War on Drugs, and also a long-standing struggle between the state and those that desire privacy through strong encryption. If you add to this concern over control of one of mankind's most important constructs – money – then CCs find themselves amongst several of the world's most hotly contested debates; in no small part, due to their connection with illicit activity on the dark net.

Yet, some 11 years after Bitcoin was invented, CCs have not played a critical role in a Cyber War, a Cyber 9/11, or been responsible for an explosion in dark net crime that threatens society. The DFS Superintendent said of virtual currencies in a 2013 interview that 'it feels as if the major advantage they're providing is anonymity' [6]. And in evidence given in 2014, DFS was told that illicit activity using virtual currencies 'reduces or even eliminates practical barriers to entry' thereby enabling the purchase of drugs globally with 'essentially the push of a button' [7]. There is little dispute that CCs are used for criminal activity, but how useful are they really? Is anonymity their major advantage? And is purchasing on the dark net as simple as clicking a button? We take a social constructivist approach to these questions. What do the users *themselves* say of their attitudes and motivations towards the usage of CCs for illicit purposes?

We follow this introduction with a background section to highlight the importance of this topic. We examine some existing user studies of CCs and also some wider work on the dark net. This exposes the gap in the literature that we aim to address through three research questions. Methodology and ethical considerations were key to researching a sensitive subject and so we consider these aspects in detail. We then discuss our results, which are achieved through analysis of underground and dark net forum posts. Our study presents several implications for policy, before closing with the conclusion.

2 Background

2.1 User Studies

CCs are an important topic of research. The world is moving increasingly towards a digital future and the methods with which we transact have undergone more evolution in the last 100 years than the previous two millennia [8]. The very form of money is changing; from new initiatives like Facebook's Libra to the prospect of Central Bank Digital Currencies. Bitcoin emerged amongst this change, at some level in response to the Great Financial Crisis but also 'as a symptom of monetary plurality in the twenty-

first century' [9]. The control of money, the form and properties of money, the relationship of money to society; all have emerged as important topics in recent years.

Early academic interest in Bitcoin was largely technical, as the original CC seemingly delivered on a long past of cryptographic endeavour and previous attempts to build digital cash [8]. The examination of CCs focussed on issues such as their ability to scale and their security – prompting calls from several researchers for more to be done from a social perspective [10, 11, 12, 13, 14]. A number of studies of user experiences of CCs have now been conducted. One of the first surveys of Bitcoin users was a web-survey of 7500 students. Amongst that group, politics and Libertarianism were an influence for using Bitcoin, whilst novelty was more of a draw than anonymity. The study concludes that Bitcoin means different things to different people [11]. Whilst this seems a simple observation, it is telling as there is a tendency in the debate about CCs to make sweeping statements, such as that CCs are a tool for criminals. The reality is, of course, more nuanced and varied. It is only by researching different groups that we can learn of the different attitudes and motivations that invariably exist between them.

In another earlier study of 1000 users, almost half identified as Libertarian [15]. This political dimension was also identified in a 2013 investigation of Bitcoin from a semiotics perspective, which analysed archived conversations of those involved in Bitcoin. The researchers showed that Bitcoin 'provides an alternative to currencies and payment systems that are seen to threaten users' privacy, limit personal liberty, and undermine the value of money through state and corporate oversight' [16]. Many other studies have now taken place to understand user experiences and motivations for using CCs, usually employing interview or web-survey methods [12, 17, 18, 19, 21, 22]. In 2015, researchers used the Technology Acceptance Model (TAM) to organise their results; interviewees expressed concerns over ease of use, and one merchant worried about price volatility. In terms of usefulness, low cost was a major driver, with anonymity not viewed as an issue [22]. Several other studies draw similar conclusions but analysed from different perspectives, such as human-computer interaction [19, 23, 24, 25].

As well as being limited to specific groups, such as students or a country by geography, the other main similarity in all these user studies is the focus on legitimate usage. There is a gap in the literature concerning the attitudes and motivations of users of CCs for illicit purposes. This is particularly important given the security-led concerns that are expressed about CCs. This paper addresses this crucial gap by conducting the first user study of CCs from an illicit perspective, in order to contribute to the debates about their existence. Furthermore, several of the studies discussed took place prior to 2017 when CCs gathered mainstream attention. This study contributes to recent knowledge of views up to late 2019.

2.2 Dark Net Studies

Usage of CCs on the dark net is an oft-cited concern yet none of the user research discussed so far addresses this issue. The dark net is a rich area of study but, again, the use of CCs on them is a largely neglected subject. Although there is a suggestion that 'cryptomarkets' will increase the volume of illegal substances for sale, researchers challenge the assumption that this will only increase harm [26]. Drug quality can be higher

and physical violence lower on dark net markets [27]. Policy makers must give careful thought to the dark net, as the effects of it are not universally negative.

Another interesting study reveals that the risk of arrest is also reduced on the dark net; there were only 391 arrests worldwide up to December 2016 [26]. This is a modest figure and should be borne in mind in relation to the findings of Kethineni, Cao and Dodge [28], who conclude, in their work applying space transition theory to Bitcoin usage on the dark net, that a lack of deterrence is one attraction of the internet to criminal behaviour. Indeed, research suggests that trade on markets increased after media coverage of successful law enforcement action on the Silk Road [29]. The research community notes that there is a lack of work assessing the effectiveness of strategies towards illicit markets [30]. Is it that CC properties enable dark net activity or is the problem more due to a lack of deterrence? Interestingly Bancroft and Reid [31] note, with regard to dark net anonymity, that this property is not a precondition for internet drug selling as drug trading exists on the internet without attempts to hide identity.

The dark net has proven to be a popular area of research for social scientists. A significant part of the literature focusses on the drugs dimension, in reflection of the status of this topic in wider society. This study adds to this knowledge with a focus on the payment mechanism, which is seldom discussed. It is important for policy makers to understand the role that CCs play on the dark net, as they consider the risks they pose.

3 Research Questions

This research seeks to explore attitudes and motivations towards the use of cryptocurrencies. To do this, we aimed to carry out the first user study of cryptocurrencies (CCs) for illicit activity, from the perspective of underground and dark net forum users. We do not seek to make any moral or legal judgement on the actions of any individuals but use the term 'illicit activity' as other researchers have done [32], as a collective term to aid discussion of a variety of actions on the internet, such as buying illegal drugs on a dark net market. The following three sub-questions were chosen in support of our aim:

Q1. What properties of cryptocurrencies are important to users for illicit activity?
Q2. What are users' attitudes and experiences of using CCs for illicit activity?
Q3. To what extent are CCs an enabler of illicit underground and dark net activity?

4 Research Method

4.1 Data Collection Method

In Gehl's field guide for studying the dark net [33] the author implores for more 'humanistic inquiry' and provides advice based on many years of studying this location of research. Gehl notes that ethnographic work on the dark net has mainly focussed on marketplaces and not on other sites, such as 'forums and social networking sites' [33]. These forums are places where discussion about the dark net takes place, including how to use the system [33]. This includes discussion of cryptocurrencies, as the main

payment method of the dark net. This study explores the attitudes and motivations towards the usage of cryptocurrencies and so forums and social networking sites were chosen as the most suitable research targets. Of particular relevance here, in terms of illicit activity, are underground forums on the internet (such as hacker sites) and forums on the dark net which require specialist software (such as the Tor browser) to access.

There are two broad strategies used by researchers to gather information on forums. The first is active engagement with users; however, this comes with significant ethical and practical implications but also with greater potential risk to participants and even researcher safety [34]. The second broad strategy is without active engagement. This can involve a bespoke scraping (downloading data) of target websites but there are also repositories of these scrapes available for research use. Considering researcher reflectivity and positionality, we selected using a repository of scraped data as the most appropriate strategy, as there were no advantages to the other methods for this study.

4.2 Sample Selection

There are a number of scraped datasets available for research. Gehl describes one 50GB source covering dates between 2011-2015 [33]. Another extensive dataset called CrimeBB has been assembled by Cambridge University's Cybercrime Centre (CCC). This dataset has been professionally curated and covers a more extensive period. For these reasons, it was chosen as the sample for research. CrimeBB was created in recognition of the fact that prior research had relied on insufficient and out of date datasets [35]. Furthermore, underground forums provide a place for criminals to discuss and exchange information, products and services – as such, they help researchers better understand 'behaviours of offenders and pathways into crime' [36].

CCC makes CrimeBB available to other researchers 'under a legal agreement, designed to prevent misuse and provide safeguards for ethical research' [35]. The dataset continues to grow as more forums are included. In 2019, CrimeBB had data from fifteen underground forums, such as Hackforums which is the largest of its kind in the English language [37]. CrimeBB also includes dark net forum data. As such, the dataset is one of the largest available to researchers, covering a wide timespan and a variety of different internet and dark net forums. Several research papers are connected to the CrimeBB dataset [33, 34, 35, 36, 37, 38, 39].

4.3 Data Analysis

The first task was to download a SQL dump for each forum available from CCC. These were then restored in a Postgres database. In total, data from 18 underground and dark net forums were added, amounting to some 100 million posts. Search terms were then employed as SQL statements to focus the relevancy of the data. Using 'Bitcoin' as an initial search term produced a selection that was still more than 200,000 posts. As a test, we coded a selection of 100 posts and found that took one hour. To code all the 'Bitcoin' posts would take in the region of one year of full-time work. Another factor that influenced selection strategy was the disparity in the size of the forum dumps. The largest forum accounted for approximately 80 per cent of the 100 million posts, whilst the smallest produced less than 100 posts containing 'Bitcoin'.

Based on the coding test and the results for each forum using the 'Bitcoin' search term, we adopted the following method to obtain our selection for coding and analysis. For any forum with more than 2000 'Bitcoin' results, 'Bitcoin' was combined with other search terms to reduce the results. For small forums with less than 2000 'Bitcoin' results, these other terms were searched for in addition to 'Bitcoin'. The effect being to widen search terms for small forums and combine search terms for larger forums.

'Bitcoin' was chosen as the 'master' search term as it is the overwhelmingly dominant CC. As the first of its type, there would also have been many years of posts where it was the only CC. To select other search terms, the 200,000 'Bitcoin' posts were then analysed using IBM SPSS Modeler's text analytics capabilities. This offers an auto-categorisation of content. By reviewing the categorisations by order of content volume, we identified new search terms of interest. We also then added a further three related terms based on experience. The following table shows the final search terms, which resulted in a total selection of 23,223 posts:

Table 1. Final Search Term Selection

Master Term	**Top 500 SPSS Categories**	**Other SPSS Categories**	**Related Terms**
Bitcoin	Money	Zcash	Dash
	BTC	Police	Feds
	Cryptocurrency	Criminal	Jail
	Monero	Privacy Coin	

The posts were then exported to Microsoft Excel. Here, 180 posts were removed as they no longer had discernible forum identifiers. Duplicates were also then removed resulting in a final 16,405 posts, equating to 164 hours of estimated coding time. Coding is central to most qualitative data analysis and software tools are often used to assist [42]. We attempted to use Nvivo but found that it took too long to process codes. After considering other options, QDA Miner Lite was selected for coding and analysis.

5 Ethics

Ethical considerations were central to the design of this study, as sites of illicit activity need extra consideration for participants and researchers. There is a risk of personal harm and also the potential to stray into illegal activity [34]. Using CrimeBB minimised many risks. The ethical principles of the Association of Internet Researchers (AoIR) were also used to assess the implications of the research conducted in the study [43]. A key point raised by AoIR is about expectations of privacy. This is a contested issue but a widely held position is that 'informed consent is not legally required to access data from publicly available forums, as they are in the public domain' [44]. There has been extensive research on internet forums, and of CrimeBB, so we did not seek informed consent. Other significant considerations highlighted by AoIR were minimised in this study. There was no interaction with any individuals from the dataset, which alone eliminated a great deal of risk and negates the need for a communications strategy.

The guidance of the British Society of Criminology (BSC) [45] also informed the methodology. Even though forums are public, information gained from the internet 'should always be critically examined and the identity of individuals protected unless it is a salient aspect of the research' [45]. This research aims to explore group behaviour and usage of cryptocurrencies, it is not necessary, therefore, to identify users by their usernames. Furthermore, the British Sociological Association [44] advises that data from online forums should not be copied verbatim. This research abides by the guidance of both organisations and does not present usernames or verbatim quotations.

BSC provides further ethical guidance concerning the law and obligations for researchers. In the UK, individuals (including researchers) are not legally obliged to report crimes they witness to the police unless an act relates to terrorism, child abuse or money laundering [45]. The nature of the data analysed here was unlikely to relate to the first two categories. One advantage of using a professionally curated dataset is that images are often removed as part of the scraping process. This reduces the chance of viewing certain types of data. The obligation with regards to money laundering relates to the Proceeds of Crime Act 2002 and relates primarily to the regulatory sector [45]. An ethics note by the University of Sheffield also comments that most information collected by researchers is likely to amount to intelligence or hearsay – it is not 'hard proof of criminality' [46]. There was, therefore, a negligible chance that this research revealed anything that would cause concern with respect to the obligations mentioned. However, if that likelihood had occurred then the protocol would have been to discuss any material with University staff before taking further action. A full ethics review of this study was approved by the University's Research Ethics Committee.

6 Results and Analysis

Neither usernames nor verbatim quotations are used in this paper. In this section, where a specific post from CrimeBB is discussed, we use the term 'author' generically in lieu of any username connected to a post.

6.1 It's About Finality, not Anonymity

Cryptocurrencies present a user with an alternative financial system with differentiated properties. Among the key properties are anonymity (or pseudonymity), speed, low-cost (usually), decentralisation (no third-parties), self-sovereignty, immutability of the blockchain and finality [8]. We define finality here as a payment transaction that, once made, cannot practically be undone. For the university students surveyed by Bashir, Strickland and Bohr [11], there was a political motivation towards usage and novelty was a greater draw than anonymity. But how does this view change amongst different user groups with different needs and wants? Specifically, which properties were most important for adoption of cryptocurrencies by underground and dark net forum users?

Whilst anonymity *generally* is important to those conducting illicit activities, it was the property of finality that emerged strongly from the coding. Many authors spoke of difficulties with using traditional finance and discussion about PayPal, in particular, was of note. It is difficult in a predominantly qualitative work such as this to

quantitatively support what, at a certain level, is something of a subjective judgement that arose from analysing the posts. However, some key search terms were submitted into QDA using the text retrieval function in order to give the reader a sense of the frequency that certain terms appeared in the 16,405 posts, as shown in Table 2.

Table 2. Total number of posts containing the selected search term

Search Term	**Number of Posts with Hits**
Anonymity	396
Anonymous	776
Pseudonymous	23
PayPal	3325
Chargeback/Charge back	333 (123/210)
Privacy coin	109
Monero/XMR	1337 (993/344)
Dash	238
Zcash	130
Verge	53
Decentralised/Decentralized	360 (54/306)
Speed	1233
Cost	855
Immutable	11
Libertarian	27
Cypherpunk	3

The meaning derived from this table is crude, but it is useful in discussion of the properties that were important to the users of this study. Of note, there was very little discussion observed of the Libertarian or Cypherpunk ideals that are often mentioned in connection to CCs. The other figures from Table 2 need to be handled cautiously. Some terms, like 'speed' and 'cost', appear relatively frequently but may have been used in many different contexts among the posts. Others, such as 'decentralis(z)ed', were present in many 'generic' posts that served as introductions to CCs. In contrast, the difficulty that many users had with traditional finance stood large as a theme in its own right. The term 'chargeback' is singular in its meaning compared to 'cost' for example, which caused it to emerge, along with 'PayPal', as significant codes of interest. Notably, neither of these terms were used in the initial filtering of posts from CrimeBB.

In 2014, PayPal extended the time to raise a dispute from 45 to 180 days. The feeling among many authors on CrimeBB was that this was great for scammers and terrible for sellers - the issue being that a trade could be made, only for a buyer to complain later causing accounts and funds to be frozen. Furthermore, the view was that third parties tended to side with the buyer rather than the seller. The result was that many people looked for alternatives without chargebacks – Bitcoin was one of several useful solutions. In 2014 when Bitcoin was relatively unknown, there were sellers considering accepting only Bitcoin despite the fear of losing most of their customers by rejecting more accepted payment methods. It is also important to note that this issue was not

limited to illicit activity - a lot of this discussion took place on the underground forums, even as far back as 2012 where authors had problems using Liberty Reserve. Discussion also highlighted some of the other reasons why people were frustrated with traditional finance and sought alternatives: PayPal, for example, is not supported in every country, under 18s are restricted from many financial services and others talked of their problems using existing services after having had previous financial difficulty. All these experiences led to the adoption of Bitcoin (primarily) as a tool open to all.

One limitation of CrimeBB is the periods covered. Underground forum posts are from as early as 2010, whilst the dark net forums date from 2014 onwards[†]. We are not, therefore, able to see dark net posts from the very early days of Bitcoin or indeed of the Silk Road era. However, there is a crossover from the underground forums where these matters are discussed. Much is also known of the dark net and the Silk Road from these times from existing research, where Bitcoin was long established as a payment mechanism for trade. And it was and is the finality of transactions that has been at the heart of Bitcoin's acceptance for illicit activity as it overcomes one of the difficulties of the internet – that of trust. As one author puts it, there is little trust on the internet. Another urges others to trust in cryptography over anything a human might say. Finality, with an immutable public ledger, enabled trust to increase, above that of the alternatives that existed at the time. Authors note that they could verify funds had been sent and be secure knowing they would not suffer chargebacks or other problems - a situation enhanced further with escrow and eventually multi-signature transactions.

The volume of posts, and their strength and tone, caused finality to emerge as the most useful property of CCs. This finding aligns with Anderson's paper pre-dating Bitcoin that 'reveals that revocability is more important' than traceability for online fraudsters using 'nonbank payment services' [47]. Speed was not a top concern in our sample when, in the case of purchasing drugs on the dark net as an example, packages were to arrive by post. Reduced cost of transactions was an attractive feature, but lower down the order than the benefits of finality. The other structural characteristics of Bitcoin contribute to achieving this benefit but were not the overt reason why it was adopted – finality solved real problems of existing alternatives. But what of anonymity? Was this not the main advantage of Bitcoin and cryptocurrencies as many believe?

6.2 Anonymity Isn't Everything

Table 2 shows that anonymity is a frequent term in posts. The dark net forums, in particular, are dense with discussions about operational security, or how not to get caught. A first important point authors note is that complete anonymity is impossible to achieve – the best that can be hoped for is sufficient security to be practically safe. Secondly, anonymity is achieved through a raft of measures, not solely through one method such as the payment mechanism. A layering of protection is needed to create obscurity. (There will be more on this in the following sub-sections). These are important distinctions, as anonymity is not, therefore, the 'main advantage' offered by CCs. They can aid in the endeavour but do not solve the issue in its entirety.

[†] One of the foreign language dark net forums has posts as far back as 2012.

Analysis of CrimeBB is also interesting from a longitudinal perspective, as we observe the changes in attitude and behaviour towards CCs. It also reveals the spectrum of user knowledge about the properties of CCs and how to use them for illicit activity. There is strong evidence from 2011/12 that many users believed that Bitcoin was fully anonymous. They were likely using the Silk Road thinking that tracking or any form of identification was not possible. Despite this, there were other users, as early as 2012, who were aware of the pseudonymous nature of Bitcoin. In one such post, an author expresses his exasperation that others keep claiming that Bitcoin is completely anonymous. There is a clear difference in understanding between those that are technically savvy and well-read, and those who are not. To those that are not, there was a belief that Bitcoin was as anonymous as cash and served that purpose as 'cash on the internet'. Posts show that users felt it was anonymous as they did not have to provide a genuine name when creating a wallet.

By 2014, the underground forums evidence a widespread recommendation to use third party 'tumbler or mixer' services with Bitcoin as the prevailing method to increase the obscurity of any trail. Ultimately though, as one author explains, Bitcoin is only as anonymous as the individual behind it. Despite this, claims of Bitcoin's complete anonymity continue through all years, as well as posts of disbelief at this lack of knowledge. Remarkably, in 2019 there is even evidence that users were buying CCs on regulated exchanges with real-world details and then sending funds directly to illicit sites. There is a noticeable difference between the underground and dark net forums in these matters. In general, the dark net forums are heavily dominated by operational security discussion and so are much more aware of the issues and take them more seriously. This makes sense and Tor appears to filter some of the banality that the easier access of underground forums enables.

Using tumblers continued to be a widespread practice from 2014 to 2016. After this time, however, users moved away from this method, citing trust (some services have control of your funds and can disappear with them) and also efficacy – you may be mixing your 'dirty' coin and receiving another 'dirty' coin in return. In 2017, one of the main tumblers closed their services as they changed their philosophy, realising that Bitcoin was intended as a transparent system. This change also aligns with the other significant development of this time, which was the emergence of privacy coins, designed with enhanced anonymity in mind in comparison to Bitcoin.

Table 2 is again a useful reference at this point. Dash, or Darkcoin as it was previously known, had some prominence in the 2014-15 period but posts show that users moved from it, questioning if its technology enabled any more security than Bitcoin. Instead, it was Monero that emerged as the most talked-about privacy coin of choice. By 2018, there was a marked clamour about the use of Monero, with some proclaiming it the rescuer and future of dark net markets. This is supported by Monero's daily transaction chart, which has been on an upward trend since early 2019 and now regularly records more daily transactions than the peak of the 2017 bubble [48]. Despite the increased security on offer from Monero, Bitcoin retains its prominence even on dark net markets. Why is this the case? That is exactly the question that many authors pose. In 2018, one author commented that Monero was not an option on many markets. A 2019 post notes that Bitcoin is awful for anonymity or privacy. It also becomes noticeable at

this time that there is anger towards Bitcoin as users cannot understand why anyone would use it for illicit activity when it has a traceable, public ledger. There are even outright calls and advice to stop using it on the dark net. Others thought it obsolete in terms of the privacy it offers and even described it as terrible for illicit activity.

Several explanations arise. Firstly, there are the network effects that Bitcoin has achieved. It is *the* CC that is universally available and accepted. People have also learnt how to use it over 11 years of operation. One seller questions the ability of buyers to use a new currency (Monero), suggesting it would be easier to accept Bitcoin and take responsibility for anonymity as part of their own operational security. Another user explains that there is no cyber law enforcement in their country, meaning there is nothing to worry about if using Bitcoin. This question of deterrence also emerges in many other posts. The widespread opinion is that law enforcement only cares about large dark net participants – if you are a buyer of small quantities then again Bitcoin will probably do. Similarly, another author states that major criminals do not need Bitcoin and that it is a poor tool for money laundering. Some other users fall into the categories of careless, misinformed, stupid, entrenched and even lazy, as author explanations for the continued use of Bitcoin. Additionally, Monero is viewed as harder to get and to use than Bitcoin. Users also worry that a connection to Monero looks suspicious. In a 2019 post, another author asks why anyone would use Monero, as none of the markets had multi-signature transactions – leaving participants to run the risk of market exit scams. One final post gets to the crux of the issue – the main advantage of Bitcoin is not anonymity.

That Bitcoin is still widely used even though it is common knowledge that it does not offer strong anonymity is prima facie evidence that this is not the main advantage on offer. To return to a point made earlier, anonymity is not and should not be sought from one element of activity. It takes many aspects of operational security to achieve sufficient anonymity – that is, a transparent currency can be used for an illicit payment as long as other countermeasures are used. For example, a user could acquire a currency with fraudulent details; in this case, it does not matter that the transaction is not anonymous. And so it is with Bitcoin and CCs. The payment mechanism is only one part of a whole set of other considerations that work to achieve the desired anonymity. It is not singularly important for Bitcoin to be anonymous – if it was, it would not be used. In this way, we can say that dark net markets are not dependent on CCs or a perceived advantage of anonymity. They can survive without this necessity.

How, though, is this possible? The following sub-sections will explore this in more detail. For now, we can summarise that illicit activity requires an overall level of anonymity, but this is not achieved through Bitcoin or a privacy coin. In this way, Bitcoin can be pseudonymous and still be used, as long as other methods are employed. Privacy coins enhance anonymity, but they are still not a singular solution. Countless posts (amongst those that care) take place on underground and dark net forums discussing how to best transact. This will now be examined.

6.3 The Payment Mechanism

The payment mechanism used to conduct illicit activity is just one of a suite of considerations that a conscientious user must scrutinise if they hope to achieve a sufficient

level of operational security. To aid discussion of this, we propose an Operational Security Taxonomy for Illicit Internet Activity, shown in Fig. 1. As the reader can see, there is a great deal to consider if you seek to conduct illicit activity as securely as possible. The seven areas of security are not exhaustive but capture the main elements that contribute towards relative anonymity. The dashed boxes are also not exhaustive but illustrate some of the considerations in each area. At the top, there is a cross-cutting theme of 'procedures', which applies to all seven security areas. For example, a procedure may be implemented to erase all hard disks weekly, or in relation to shipping to ensure that a home address is free of illicit material prior to an expected delivery.

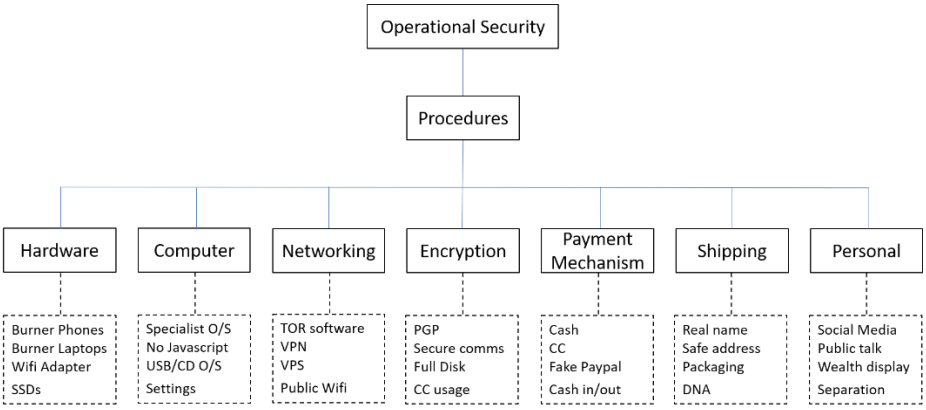

Fig. 1. Operational Security Taxonomy for Illicit Internet Activity

Our focus here is on the payment mechanism. We begin with the following claim – banning CCs would not materially reduce illicit internet activity. In many areas of the taxonomy, we can think of there being 'tools for the job'. The history seen through CrimeBB shows that when one payment mechanism falls, another is quickly found. When Liberty Reserve ceased, other options were soon adopted. As difficulties with traditional finance grew, demand for Bitcoin increased. And now, as Bitcoin is scrutinised, many want to move to Monero. There are always alternative payment mechanisms. Table 3 highlights some of those used in CrimeBB.

Table 3. Selection of Payment Mechanisms in CrimeBB

Payment Type	**Example Mechanisms**
Cryptocurrencies	Bitcoin/Litecoin/Monero/Dash/Zcash
Payment Processors	PayPal, Western Union, MoneyGram, Skrill (Moneybookers), Payza, Webmoney, Moneypak,
Bearer Assets	Cash, Gift Cards
Fintech	Perfectmoney, Cashapp, Venmo, Greendot, Dwolla, Perfectmoney, UKash, Virwox, Paysafecard
Gaming Currency	Runescape Gold, Second Life Linden Dollars
Traditional Finance	Bank Account, Credit/Debit Cards, Prepaid Debit Cards, Polish Bank Cards

The table shows that a ban on CCs would only restrict one potential mechanism, leaving several other options. If we consider just the bearer type, we see that it is an ultimate recourse should every other type become unavailable. Bearer assets are owned by the holder and so offer a finality of transaction, like CCs. Cash is the most common example and finality explains why 'cash is still king' for criminal transactions [8]. Indeed, as several authors point out, cash is the main mechanism for purchasing drugs more widely. Another author describes successfully sending cash through the mail system – established techniques such as this would be extremely difficult to counter and exist as proven payment mechanisms should other methods disappear. Gift cards are another readily available bearer mechanism discussed and used in a multitude of posts.

Several authors question the logic of a ban on CCs. They view cash as being a greater enabler of criminal activity than CCs and believe there is a hypocrisy in targeting CCs over cash or the traditional financial system. Authors acknowledge that CCs are used in crime but ask if that is different from any other payment mechanism. It is worth noting at this point the central role that cash also plays in illicit internet activity. Not only is it used as a payment mechanism, it also acts as a fundamental tool for achieving anonymity. One of the most discussed topics, particularly on the dark net forums, is the subject of 'cashing in or out' of CCs. As CCs are still a relatively small market and not accepted widely in the world, authors describe the need to transfer any CCs into and out of cash for use in the real world. In this way, cash can often be thought of as the anonymity wrapper applied around a pseudonymous Bitcoin transaction. This again explains why anonymity is not the main property needed from CCs as an illicit payment mechanism - as long as anonymity can be achieved elsewhere as part of the process.

In fact, the increasing difficulties of cashing in/out, arguably brought on by improving regulation of legitimate CC services, has deterred some illicit activity. One author describes being put off from selling on the dark net due to this difficulty of cashing out. There is a further interesting paradox to consider about the efficacy of bans. Currently, most illicit transactions have a connection to legitimate services. This brings opportunity for enforcement. However, a ban would likely push users to illicit mechanisms and reduce some of these opportunities. Cash can be sent in the mail or deposited into a bank account. Or legitimate mechanisms would be used fraudulently, such as registering for services using fake identification. These methods are harder to stop and arguably leave less opportunity for enforcement. In this way, a ban would reduce opportunity for legitimate users and merely push illicit activity towards other established mechanisms that are harder to control. Dark net market activity would be temporarily affected but users would likely soon find alternatives, as they have done after Liberty Reserve ceased or the repeated closure of markets themselves. Legitimate services drain liquidity away from illicit methods, making them rarer and harder to use.

Finally, policy makers must consider whether they could even achieve a ban. The nature of CCs means that they cannot be shut down as easily as a centralised service like Liberty Reserve. And as long as a decentralised CC system persists, there is little that can be done about individuals meeting in the real-world to trade CCs for cash, for example. As one author puts it, criminals could still use Bitcoin if it was banned and only ordinary users would be affected. Another writes that Bitcoin is simple for

legitimate activity but hard for illicit. Regulated exchanges combined with a transparent record of transactions make illicit payments harder. On this point, an author writes that analysis of the Bitcoin blockchain has been central to all dark net market prosecution and that, if you use Bitcoin, you must ensure that every aspect of your operational security is infallible. In another post, the author decries the hype around CCs or that they are revolutionary to simply say that they are just a useful tool to transact with, like other monies. CCs are, then, useful for illicit activity as they are a useful payment mechanism. But it is too simple to say they are 'great' for criminals - there is far more to consider in terms of their usage. They are a tool among many, as the taxonomy shows, but as an individual mechanism, they come with significant disadvantages to the illicit actor.

6.4 Dark Nets are Hard

A recent research paper that also analysed CrimeBB came to the conclusion that 'cybercrime is (often) boring' [41]. To this, we add that cybercrime, particularly on the dark net, is hard. The dark net is fraught with risk – scammers abound, and law enforcement action has been successful to an extent. The taxonomy shows that there is a significant educational and technical barrier in order to illicitly transact relatively securely on the internet. Even for a careless user, the minimum required to use the dark net is a computer with Tor set up, a delivery address and a working knowledge and possession of CCs. We contend, therefore, that dark net markets are a niche and are unlikely to grow significantly in comparison to traditional counterparts. The dark net may reduce risk in acquiring narcotics, for example, but it is arguably much easier, as some of the authors claim, to get cash and buy drugs in the real-world. Dark net markets only cater for a small volume of overall crime [8] – the threat should not be overexaggerated.

There are countless guides and posts on the underground and dark net forums discussing how to conduct illicit transactions. Even just the payment mechanism part of the taxonomy requires substantial knowledge. Users must also keep up with changing methodologies as services come and go, regulation tightens, and behaviours evolve. One author describes studying for many months before being able to start selling on a market. Another author tells of mental exhaustion from researching how to buy. The author thought it would be simple, perhaps as easy as 'pushing a button' - the reality was the opposite. There is no better example of this than the Dark Net Market's Buyer Bible [49]. This is a guide written for users wanting to purchase on dark net markets – it is 133 pages long. We cannot discuss the Bible or the taxonomy in full detail from a buyer's or seller's perspective as it would be too long but here follows a few items that highlight some of the complexity involved: use a non-windows, Linux based machine for a specialist operating system such as Tails or Whonix on a portable media (USB/CD), acquire a VPN service anonymously, learn to use PGP for encryption, use pre-installed IP tables as needed, disable JavaScript in the browser, get onion addresses from a reputable website, use a self-destructing messaging service, acquire BTC using cash from an ATM using a disguise and burner phone, convert Bitcoin to Monero using a non-exchange wallet… Advice for sellers is even more exhausting.

This also shows why privacy coins are not a panacea for anonymity. The user must acquire the Monero, for example, most probably with Bitcoin. Websites exist to

highlight services such as VPN providers and decentralised exchanges that aid in anonymity [50]. For example, a popular service on CrimeBB is xmr.to, which will send Bitcoin to a recipient in exchange for Monero. Or morphtoken.com which exchanges cryptocurrencies e.g. Monero for Bitcoin. However, even with these tools a user still needs to cash in/out, plus do every other part of the taxonomy securely. It is a difficult task.

We must also consider the environment of the dark net itself. One user from the early days commented on how much more difficult it had become. Whilst there was early disdain about law enforcement capability, authors now acknowledge much improvement since the Silk Road market. There is evidence of some fear of law enforcement activity. However, an author notes in 2014 that arrest is more likely in the real-world. As such, the view remains that buyers of small amounts have little to worry about. The extent of deterrence on the dark net is therefore limited. Operation has become more difficult, but buyers do not think there is much chance of law enforcement interest in their activities. The role that Bitcoin analysis has played in prosecution is known but sellers continue, believing that they can operate if they take sufficient precaution. Recent views from 2019, though, show that marketplaces are hard to trust and often disappear after short periods. This all leads to a sense of containment if nothing else, as authors hope for improved days based on innovation using new technologies. The desire for a truly decentralised marketplace using Monero is there to see. There is a paradox here, that every law enforcement success leads to a Darwinian hardening of the system, which one day could leave little in way of enforcement opportunity.

To finish this section, we consider the words from three final posts. One author reminds readers that even if you do everything right (according to the taxonomy), using the dark net still requires trust and 'hope'. Hope that someone else has not done something to compromise your security, such as a seller that is caught who has not deleted customer addresses. Another reminds that people make errors and security cannot be applied retrospectively. You must get everything right from the beginning, which is difficult and can lead to silly mistakes getting you caught (as in the case of Ross Ulbricht). This leads us to the final comment, that the dark net appears to be easy and safe to use – but it isn't. It is a risky domain and it requires a lot of research and capability to use it relatively securely. And for these reasons, it is not for everyone.

7 Discussion

7.1 Implications for Policy

This paper challenges the notion that the main advantage of using CCs for illicit activity is anonymity. Users adopted CCs because they were a useful tool that solved real-world problems. Finality was the property most sought. Policy makers should recognise the issues people had that led to this adoption. It is important that traditional systems are inclusive and fair to all; they should not drive users to alternative choices.

Banning CCs is unlikely to do more than disrupt illicit internet activity. If anything, this reduces opportunity for legitimate use, pushes liquidity to illicit methods and reduces law enforcement opportunity by reducing contact with regulated systems. There

are many other payment mechanisms that could be used for illicit activity; some, such as cash, are even harder to monitor than CCs. A ban would also likely be ineffective due to the decentralised nature of CC systems.

Law enforcement action has contained dark net activity and created a degree of deterrence, but little at the small buyer level. For these buyers, research shows that the dark net may reduce harm. Policy makers must also consider the evolutionary nature of markets and the impact that future technology could have on law enforcement impact.

Illicit internet activity is hard to achieve relatively securely, as the taxonomy shows. Dark net markets are therefore a niche and are unlikely to explode in size. The creators of Silk Road and AlphaBay markets were not from traditional crime groups. Policy should consider the threat that the dark net measurably poses and react accordingly. There is a danger that headlines make it seem more of a threat than it is. It is unlikely that dark net markets will capture significant shares of real-world counterparts.

7.2 Limitations

CrimeBB covers limited periods for each forum, meaning there is a wide range in the amount of material available. It is, though, a fantastic resource and our thanks go to CCC for their efforts in making this dataset available. It reduces many problems associated with research in this domain.

Particular care was taken in choosing search terms and using a content analysis method enabled themes to emerge naturally. As a qualitative study, we do not claim to 'prove' our findings but justify them based on the reading that emerged. We would have liked to have used quotations from posts to show the discussions that led to our results, but our ethical guidance advised against this. CrimeBB is, of course, available to other researchers should they wish to know more or to reproduce the results.

8 Conclusion and Future Work

This research addresses a gap in the literature by conducting the first user study of CCs for illicit activity. It also adds to the research on the dark net by focussing on payment mechanisms, rather than well-researched aspects such as harm or drug availability.

We present several significant findings that have implications for policy. Anonymity is not the main advantage of CCs for this user group, finality is. This challenges established assumptions and shows the value of qualitative research in this subject. Bitcoin is not as anonymous as cash but, in many respects, has proven to be the next best thing on the internet for illicit transactions. Is it great for criminals? The answer is a predictable yes and no. Yes, in that it proved to be a useful payment mechanism, offering finality and open access to those cut off from traditional finance; in the lexicon of TAM, it had a utility that led to adoption. No, in that using CCs for illicit activity is difficult, they are traceable and the dark net itself can be an inhospitable place. Even privacy coins do not solve the anonymity problem; users must still cash in and out and must also overcome significant barriers to use CCs relatively safely, as shown by the taxonomy. Finally, banning CCs is unlikely to be effective; determined users will switch to another payment mechanism, some of which are already established and proven. Or

they will find a way to continue using CCs. The dark net is a niche; it is not an existential threat, and neither are CCs.

Society continues to wrestle with questions of liberty and security. 9/11 shifted us towards security and Snowden moved the dial back towards liberty. Debates about these issues and the question of balance between them endure - but we need to take care in our response to perceived threats [51]. Or, at the very least, continue to look for ways 'out of the impasse of security' [52]. We hope this study contributes to this aim.

References

[1] mondovisione.com, "New York State Department Of Financial Services Superintendent Remarks At Columbia Law School," 2015. [Online]. Available: https://m.mondovisione.com/. [Accessed: 30-Jun-2020].

[2] T. Rid, "Cyber War Will Not Take Place," *J. Strateg. Stud.*, vol. 35, no. 1, pp. 5–32, Feb. 2012, doi: 10.1080/01402390.2011.608939.

[3] K. Zetter, "FBI Fears Bitcoin's Popularity with Criminals," *Wired*, 2012. [Online]. Available: https://www.wired.com/2012/05/fbi-fears-bitcoin/. [Accessed: 09-Jan-2019].

[4] M. M. Shi, "Fed Chair: Cryptocurrencies Are 'Great' For Money Laundering," *Coindesk*, 2018. [Online]. Available: https://www.coindesk.com/fed-chair-cryptocurrencies-are-great-for-money-laundering. [Accessed: 09-Jan-2019].

[5] A. Rappeport and N. Popper, "Cryptocurrencies Pose National Security Threat, Mnuchin Says," *The New York Times*, 2019. [Online]. Available: https://www.nytimes.com/2019/07/15/us/politics/mnuchin-facebook-libra-risk.html. [Accessed: 31-Jul-2019].

[6] G. Farrell and E. Larson, "Lawsky Says 'So Be It' If Transparency Harms Bitcoin," *bloomberg.com*, 2013. .

[7] US Department of Justice, "Department Of Financial Services Hearing On Law Enforcement And Virtual Currencies," 2014. [Online]. Available: https://www.justice.gov. [Accessed: 30-Jun-2020].

[8] S. Butler, "Criminal use of cryptocurrencies: a great new threat or is cash still king?," *J. Cyber Policy*, vol. 4, no. 3, pp. 326–345, Sep. 2019, doi: 10.1080/23738871.2019.1680720.

[9] N. Dodd, "The Social Life of Bitcoin," *Theory, Cult. Soc.*, vol. 35, no. 3, pp. 35–56, 2017, doi: 10.1177/0263276417746464.

[10] H. Karlstrøm, "Do libertarians dream of electric coins? The material embeddedness of Bitcoin," *Distinktion J. Soc. Theory*, vol. 15, no. 1, pp. 23–36, Jan. 2014, doi: 10.1080/1600910X.2013.870083.

[11] M. Bashir, B. Strickland, and J. Bohr, "What motivates people to use Bitcoin?," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016, vol. 10047 LNCS, pp. 347–367, doi: 10.1007/978-3-319-47874-6_25.

[12] S. Abramova and R. Böhme, "Perceived Benefit and Risk as Multidimensional Determinants of Bitcoin Use: A Quantitative Exploratory Study," *Proc. Thirty-Seventh*

Int. Conf. Inf. Syst. (ICIS 2016), pp. 1–20, Dec. 2016.

[13] A. Alshamsi and P. P. Andras, "User perception of Bitcoin usability and security across novice users," *Int. J. Hum. Comput. Stud.*, vol. 126, pp. 94–110, Jun. 2019, doi: 10.1016/J.IJHCS.2019.02.004.

[14] A. Hayes, "The Socio-Technological Lives of Bitcoin," *Theory, Cult. Soc.*, 2019, doi: 10.1177/0263276419826218.

[15] J. Bohr and M. Bashir, "Who Uses Bitcoin? An exploration of the Bitcoin community," in *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, 2014, pp. 94–101, doi: 10.1109/PST.2014.6890928.

[16] B. Maurer, T. C. Nelms, and L. Swartz, "'When perhaps the real problem is money itself!': the practical materiality of Bitcoin," *Soc. Semiot.*, 2013, doi: 10.1080/10350330.2013.777594.

[17] I. Roussou and E. Stiakakis, "Adoption of Digital Currencies by Companies in the European Union: A Research Model combining DOI and TAM," in *4th International Conference on Contemporary Marketing Issues*, 2016.

[18] F. Shahzad, G. Xiu, J. Wang, and M. Shahbaz, "An empirical investigation on the adoption of cryptocurrencies among the people of mainland China," *Technol. Soc.*, vol. 55, pp. 33–40, Nov. 2018, doi: 10.1016/J.TECHSOC.2018.05.006.

[19] J. C. Mendoza-Tello, H. Mora, F. A. Pujol-López, and M. D. Lytras, "Social Commerce as a Driver to Enhance Trust and Intention to Use Cryptocurrencies for Electronic Payments," *IEEE Access*, vol. 6, 2018, doi: 10.1109/ACCESS.2018.2869359.

[20] X. Gao, G. D. Clark, and J. Lindqvist, "Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users," *Proc. 2016 CHI Conf. Hum. Factors Comput. Syst.*, 2016, doi: 10.1145/2858036.2858049.

[21] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl, "The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy," in *Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers*, 2016, pp. 555–580.

[22] A. W. Baur, J. Bühler, M. Bick, and C. S. Bonorden, "Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of Bitcoin and Co," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015, vol. 9373, pp. 63–80, doi: 10.1007/978-3-319-25013-7_6.

[23] W. Presthus and N. O. O'Malley, "Motivations and Barriers for End-User Adoption of Bitcoin as Digital Currency," *Procedia Comput. Sci.*, vol. 121, pp. 89–97, 2017, doi: 10.1016/j.procs.2017.11.013.

[24] C. Sas and I. E. Khairuddin, "Exploring Trust in Bitcoin Technology: A Framework for HCI Research," in *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction*, 2015, pp. 338–342, doi: 10.1145/2838739.2838821.

[25] C. Tsanidis, ; Dafni, M. Nerantzaki, G. Karavasilis, V. Vrana, and D. Paschaloudis, "Greek consumers and the use of Bitcoin," in *The Business & Management Review*, 2015, vol. 6, pp. 30–31.

[26] J. Aldridge, A. Stevens, and M. J. Barratt, "Will growth in cryptomarket drug buying

increase the harms of illicit drugs?," *Addiction*, vol. 113, no. 5, 2018, doi: 10.1111/add.13899.

[27] M. J. Barratt, J. A. Ferris, and A. R. Winstock, "Safer scoring? Cryptomarkets, social supply and drug market violence," *Int. J. Drug Policy*, vol. 35, 2016, doi: 10.1016/j.drugpo.2016.04.019.

[28] S. Kethineni, Y. Cao, and C. Dodge, "Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes," *Am. J. Crim. Justice*, vol. 43, no. 2, 2018, doi: 10.1007/s12103-017-9394-6.

[29] I. Ladegaard, "We know where you are, what you are doing and we will catch you: Testing deterrence theory in digital drug markets," *Br. J. Criminol.*, vol. 58, no. 2, 2018, doi: 10.1093/bjc/azx021.

[30] T. J. Holt, "Identifying gaps in the research literature on illicit markets on-line," *Global Crime*, vol. 18, no. 1, pp. 1–10, 2017.

[31] A. Bancroft and P. Scott Reid, "Challenging the techno-politics of anonymity: the case of cryptomarket users," *Information, Commun. Soc.*, 2016, doi: 10.1080/1369118X.2016.1187643.

[32] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware Payments in the Bitcoin Ecosystem," *Pap. Present. to 17th Annu. Work. Econ. Inf. Secur. Innsbruck, Austria, 18-19 June*, 2018, doi: 10.1016/j.specom.2007.01.008.

[33] R. W. Gehl, "Archives for the Dark Web: A Field Guide for Study," in *Research Methods for the Digital Humanities*, Cham: Springer International Publishing, 2018, pp. 31–51.

[34] M. J. Barratt and A. Maddox, "Active engagement with stigmatised communities through digital ethnography," *Qual. Res.*, vol. 16, no. 6, pp. 701–719, 2016, doi: 10.1177/1468794116648766.

[35] S. Pastrana, D. R. Thomas, A. Hutchings, and R. Clayton, "CrimeBB: Enabling Cybercrime Research on Underground Forums at Scale," in *Proceedings of the 2018 World Wide Web Conference (WWW '18). Republic and Canton of Geneva, Switzerland*, 2018, pp. 1845–1854, doi: 10.1145/3178876.3186178.

[36] A. Caines, S. Pastrana, A. Hutchings, and P. J. Buttery, "Automatically identifying the function and intent of posts in underground forums," *Crime Sci.*, Dec. 2018, doi: 10.1186/s40163-018-0094-4.

[37] S. Pastrana, A. Hutchings, D. Thomas, and J. Tapiador, "Measuring eWhoring," in *Proceedings of the Internet Measurement Conference (IMC '19). ACM, New York, NY, USA*, 2019, pp. 463–477, doi: 10.1145/3355369.3355597.

[38] D. R. Thomas, S. Pastrana, A. Hutchings, R. Clayton, and A. R. Beresford, "Ethical issues in research using datasets of illicit origin," in *IMC '17 Proceedings of the Internet Measurement Conference. Association for Computing Machinery (ACM), New York, NY*, 2017, pp. 445–462.

[39] S. Pastrana, A. Hutchings, A. Caines, and P. Buttery, "Characterizing eve: Analysing cybercrime actors in a large underground forum," in *21st International Symposium, RAID 2018, Heraklion, Crete, Greece, September 10-12*, 2018, vol. 11050 LNCS, doi: 10.1007/978-3-030-00470-5_10.

[40] A. Hutchings and S. Pastrana, "Understanding eWhoring," in *Proceedings - 4th IEEE European Symposium on Security and Privacy, EURO S and P 2019*, 2019, pp. 201–

214, doi: 10.1109/EuroSP.2019.00024.
[41] B. Collier, R. Clayton, A. Hutchings, and D. R. Thomas, “Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies,” in *Workshop on the Economics of Information Security*, 2020, doi: https://doi.org/10.17863/CAM.53769.
[42] A. Bryman, *Social Research Methods*, Fourth. Oxford: Oxford University Press, 2012.
[43] A. Markham and E. Buchanan, “Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee (Version 2.0) AUTHORS,” 2012.
[44] L. Sugiura, “Researching Online Forums,” 2017.
[45] BSC, “British Society Of Criminology Statement Of Ethics 2015,” 2015.
[46] The University of Sheffield, “Research Involving Illegal Activities,” 2018.
[47] R. Anderson, “Closing the Phishing Hole-Fraud, Risk and Nonbanks,” 2007.
[48] bitinfocharts.com, “Monero Transactions Chart,” 2020. [Online]. Available: https://bitinfocharts.com/comparison/monero-transactions.html. [Accessed: 03-Jul-2020].
[49] Anon, “Dark Net Market’s Buyer Bible,” 2018.
[50] KYCNOT.ME, “Exchanges,” 2020. [Online]. Available: https://kycnot.me/. [Accessed: 29-Jun-2020].
[51] L. Amoore and M. De Goede, “Governance, risk and dataveillance in the war on terror,” *Law Soc. Chang.*, vol. 43, pp. 149–173, 2005, doi: 10.1007/s10611-005-1717-8.
[52] M. Neocleous, *Critique of Security*. Edinburgh: Edinburgh University Press, 2008.