This is a draft chapter. The final version is available in Research Handbook on International Drug Policy edited by David R. Bewley-Taylor and Khalid Tinasti, published in 2020, Edward Elgar Publishing Ltd

https://doi.org/10.4337/9781788117067

Title: Chapter 20 – Drug cryptomarket futures: structure, function and evolution in response to law enforcement actions

Authors

Patrick Shortis, Department of Criminology, School of Social Sciences, University of Manchester. (ORCID 0000-0003-3527-6667)

Judith Aldridge, Department of Criminology, School of Social Sciences, University of Manchester. (ORCID 0000-0002-9402-8682)

Monica J. Barratt, Social and Global Studies Centre, RMIT University, and National Drug and Alcohol Research Centre, UNSW Sydney, Australia (ORCID 0000-0002-1015-9379)

"There's no book on it because we are still making it up as we go along - if this was hip hop we haven't even got to the Sugarhill Gang yet."

- r/DarkNetMarkets Reddit user

Abstract

Developments in encryption technology have facilitated new forms of digital drug trading. In this chapter, we provide an overview of cryptomarkets and the technologies that underpin them. Our examination of the history of cryptomarket development shows they have evolved in response to enforcement operations and threats from within the community, yet policy responses, whilst increasingly varied and sophisticated, remain in line with prohibition and suppression. Our evaluation of the transformative potential of cryptomarkets on the global drugs trade suggests it is limited to specific drugs, countries and forms of violence, and its impact will be greater in countries where drug consumption is highest rather than producer countries like Colombia or Afghanistan. Whilst the literature is emergent, we argue that it demands better scrutiny from law enforcement and policy makers in designing appropriate responses to the online drugs trade to avoid unintentionally increasing harms both for drug takers and the public.

Keywords: (1) Cryptomarkets (2) Darknet markets (3) Illegal drugs (4) Drug markets (5) Law enforcement (6) Cybercrime

Introduction

Since cryptomarkets came into public purview in 2011, they have provided some excellent lessons for how the disruptive potential of technology can interact with the drugs trade. Over the last eight years, cryptomarkets have evolved quickly in the face of internal threats posed by malicious actors within their community and the external threat of law enforcement action. Current policy approaches favour disrupting the cryptomarket trade in much the same way as offline drugs markets to further prohibitionist objectives, yet such action seems premature given

that the emerging body of evidence suggests differentials in harms and benefits unique to cryptomarkets in comparison to real-world drug markets. This chapter provides an overview of cryptomarkets and how they have evolved since their inception, as well as how law enforcement tactics have changed over time. We shall consider whether cryptomarkets have the potential to change the global drug markets, and what impacts, if any, they might have on violence, pricing and drug purity. We will also examine the possibilities of harms and benefits that cryptomarkets bring to the global trade in drugs, and these will be shown to be ambiguous and interconnected. We conclude with some concerns about the trajectory of current policy responses to cryptomarkets, and the uncertain and possibly harmful outcomes that may result.

What are drug cryptomarkets?

Terminology and definition

Cryptomarkets are online marketplaces designed to enable anonymous buying and selling of illegal goods and services. The cryptomarket trade is dominated by illegal drugs and fraud-related products and services, such as stolen identity or credit card data. *Cryptomarket* was the original indigenously-used term in hacker forums (Aldridge and Décary-Hétu, 2014) and referred to marketplaces accessible only by using anonymising software like Tor. The term *darknet market* has now overtaken cryptomarket in indigenous, popular and often official usage, but – in common with many academic researchers – we prefer the precision and clarity offered with the term cryptomarket. We define cryptomarkets as online marketplaces: that host multiple sellers or 'vendors' in return for a commission on sales; that are accessible only via encryption software that enables buyers and sellers to transact with near-anonymity; that facilitate payment using cryptocurrencies like Bitcoin rather than using identity-linked credit or debit cards; and that display comments left by customers and aggregate their transaction feedback ratings into comparable product and vendor metrics (Barratt and Aldridge, 2016). Cryptomarkets therefore represent the subset of online marketplaces that employ encryption technologies to conceal the identity of users (Martin, 2014), as well as the subset of encrypted online selling platforms that host multiple vendors and provide third-party services, as distinct from encrypted but single-vendor shops (Persi Paoli et al., 2017). The term cryptomarket is also preferable in avoiding the problematic connotations of the word 'dark' – evil, frightening, exclusively illegal (Barratt and Aldridge, 2016). And while 'dark' has appropriately been used by criminologists to convey what is hidden – such as the 'dark figure of crime' (Biderman and Reiss Jr, 1967), cryptomarkets and cryptomarket activity, in contrast, are publicly visible.

Learning to buy and sell on drug cryptomarkets

The cryptomarket trade in illegal drugs shares much in common with legitimate e-commerce platforms found on the 'clearnet' like eBay or Amazon Marketplace (Barratt, 2012; Aldridge and Décary-Hétu, 2014). Because marketplace owners do not themselves sell goods and services, but instead host the vendors who do, their profits are derived from commissions on sales. In return, marketplace administrators (employees or owners themselves) ensure effective market function by maintaining platform security; providing collated ratings and feedback for products and vendors that prospective customers can use to guide their comparison shopping; and adjudicating in disputes as these arise. Cryptomarkets typically specify rules about which products, services and behaviours are allowed or prohibited; commonly banned products and services include child sexual abuse material, assassination services and firearms (Morselli et al., 2017). Moderators and administrators monitor marketplace activity and their associated

discussion forums to ensure compliance. Vendors depend on existing postal and delivery networks and therefore devise and share so-called 'stealth' packaging strategies designed to reduce the likelihood of interception by postal and border agents (Aldridge and Askew, 2017).[1] The similarities that cryptomarkets share with sites like Amazon or eBay make cryptomarkets familiar to users, easing adaptation to illicit online buying and selling. To use cryptomarkets, however, users must additionally get to grips with three key technologies: (1) anonymising software for accessing and using the marketplace; (2) Pretty-Good-Privacy (PGP) encryption; and (3) cryptocurrencies.

Cryptomarkets rely on anonymising software that directs internet traffic through a complex network designed to conceal a user's IP address, as well as the servers from which cryptomarkets operate. This kind of anonymity protects marketplaces owners and users alike from individuals and government organisations conducting network surveillance, including IP tracing to real-world identities (Lewman, 2016). The Tor Browser is by far the most popular and easy to use, but some cryptomarkets rely on less user-friendly alternatives like I2P[2]. Tor therefore provides a good standard of what we might term *passive* security; because Tor makes it difficult to trace marketplace activity to identifiable individuals, simply by using the cryptomarket – even in the absence of additional obfuscation methods – users' identities are concealed.

Added security is provided by PGP encryption. PGP is software that encrypts messages sent by one individual that can only be decrypted – and therefore read – by the intended recipient (Zimmermann, 1995). PGP users hold two 'keys': one public, and one private. Messages encrypted with an individual's public key can only be read using that same individual's private key. Direct communications are commonplace between cryptomarket vendors and customers; just as in legal online marketplaces like eBay, customers may request more detailed information on available products. Use of PGP encryption provides extra security; even if a message is intercepted en route to a vendor, or a market is taken over by law enforcement, the contents of messages cannot be read by anyone but the intended recipient. Many cryptomarkets actively encourage or require PGP use, particularly for messages containing information that can be traced to individuals, such as postal addresses for delivery, and research suggests that PGP use on cryptomarkets has substantially increased (Soska and Christin, 2015).

Cryptocurrencies are decentralised digital currencies that enable cryptomarket users to make and receive non-cash payments without the identity disclosures required by banks and credit card companies that operate using government-backed currencies. Cryptocurrency transactions are verified in the 'blockchain' – a public, distributed digital ledger – rather than by banks (Nakamoto, 2008). Bitcoin was the first cryptocurrency designed in 2009 by the pseudonymous "Satoshi Nakamoto", but since then there have been many variants known colloquially as 'altcoins' (Wagner, 2014). Cryptocurrencies are stored in virtual wallets, which can be acquired without providing any personally identifying information, which obscures links between their use and users (Meiklejohn et al., 2013). Cryptocurrencies can also be laundered through mixing or "tumbling" services that further obfuscate links between user wallets and intended destinations. Although Bitcoin is the most popular cryptocurrency, its ledger is public and so it is possible to trace how money flows through the network, whereas some altcoins like Monero provide better anonymity to their users (MoneroHow, 2017).

[1] There is some evidence to suggest that some vendors engage in a "dead-drop" method in which the drugs are dropped in a location which is sent to the buyer once payment is made. However the postal method is the most popular method.

[2] Whilst there are other alternative overlay networks that work differently to Tor, such as I2P, we find that Tor is by far the most popular platform for cryptomarkets at the time of writing, and therefore our discussion will mostly be focused on Tor's hidden services.

The Evolution of Cryptomarkets and Policy Responses

The link between drugs and the internet goes back to its birth, with the apocryphal tale of ARPANET's first business transaction involving a bag of cannabis (Markoff, 2005). The history of how cryptomarkets have evolved in the face of the international prohibition regime, however, goes back even further. UN conventions over the latter half of the twentieth century, such as the 1961 Single Convention on Narcotic Drugs, the 1971 Convention on Psychotropic Substances and the 1988 Convention against Illicit Traffic framed the law enforcement and policy responses to this problem long before the emergence of wide-spread encryption-based communication technologies that made cryptomarkets possible. Indeed, we argue that many of the developments in illicit drug markets within the last ten years, including the emergence of online marketplaces, flourished in the context of the international drug control regime that has focussed disproportionately on the trafficking and criminality associated with drugs such as heroin and cocaine using operations located in the crop cultivation and production countries of the Global South (Buxton, Bewley-Taylor, & Hallam, 2017). The unintended consequences of prohibition; the militarisation of law enforcement approaches to interdiction, the framing of people who take drugs as violent criminals and the risk-enhanced profits of the growing black market in narcotics are all well-documented in the literature (OSF, 2011). Over the past decade disruptive technologies have created innovations to solve problems often only understood in retrospect, and in this way cryptomarkets are not so different, solving the problems of centralised control, violence and territorial issues intrinsic to drugs with decentralised, virtual and professionalised markets. As we review the history of cryptomarkets in this section, we will see how the law enforcement strategies framed by a twentieth century prohibition regime face unique new challenges posed by a twenty-first century digital drugs market.

Whilst cryptomarkets originated in 2011 with the first market called *Silk Road*, there have been some key changes in the number of markets operating, alongside their structure and function. This section will track the evolution of cryptomarkets from 2011 up to 2019and highlight some of these changes.

2011 – 2013: The Silk Road Era

Early in 2011 the first cryptomarket *Silk Road* was launched, and in June of the same year, brought to public attention by an article in the blog Gawker (Chen, 2011). For the administrator of the marketplace – using the pseudonym *Dread Pirate Roberts* (DPR) – Silk Road was no mere criminal enterprise; it represented a vanguard libertarian development. Alongside the drugs, digital goods and other items the market offered, Silk Road's associated discussion forum provided members with a book club, and discussions on philosophy, politics and ethics. Research suggests that many in the Silk Road 'community' were not exclusively focused on buying and selling, but actively engaged in shaping codes of conduct, such as what information vendors should give to customers and which items should not be allowed for sale (Martin, 2014). Silk Road's discussion forum also provided a valued location for sharing drug harm reduction knowledge and practice (Van Hout and Bingham, 2014). In this way, Silk Road users were engaging in constructive activism that sought not only to reject drug prohibition, but also to develop a "permissive reality" towards drugs within a digital setting (Maddox et al., 2016).

In common with familiar e-commerce platforms for legal products, Silk Road was highly professionalised and service-oriented (Van Hout and Bingham, 2013). During the period in which it was active, Silk Road grew quickly. Christin (2012) estimated that between November 2011

and July 2012, the number of active sellers more than doubled, and most users were leaving the highest feedback ratings possible. Revenue generated on Silk Road for all items in 2012 was estimated to be USD $15 million, the majority of which was driven by the sale of drugs. By the time the market closed, sales revenue was estimated at USD $300,000 daily, or USD $100 million annually (Soska and Christin, 2015). While most drug transactions were consistent with 'personal use' in price/quantity, just over one quarter of all drugs revenue on Silk Road was generated by drug purchases in large quantities priced over USD $1000 (Aldridge and Décary-Hétu, 2016b). Vendors offered buyers substantial quantity discounts which were often explicitly marketed to drug dealers sourcing stock (Aldridge and Décary-Hétu, 2014). Silk Road drug vendors have been characterised as rational and informed decision-makers, particularly when compared to their offline drug selling counterparts (Aldridge and Askew, 2017). While drug vendors acknowledged the additional risks – to profit, to reputation, and risk of arrest – involved in shipping drugs across international borders (Décary-Hétu et al., 2016), the potential for high profits led vendors transacting with international customers to seek to minimise these risks by sharing good practice in connection to packaging, drop-offs for shipping, and customer communications (Aldridge and Askew, 2017). In this way the Silk Road functioned to rebalance the asymmetric advantage of information-sharing that law enforcement agencies have classically enjoyed over criminals in the past (Martin, 2014).

On 2 October 2013, FBI arrested a 29-year old Ross Ulbricht in a library in San Francisco in connection to his role as creator of the Silk Road. The investigation, dubbed 'Operation Marco Polo', saw the Silk Road site closed and the homepage replaced with an FBI seizure notice. The FBI reported that they had seized over $33 million in bitcoin from both the Silk Road and Ulbricht (FBI, 2013). Ulbricht's trial revealed that several law enforcement agencies, through taking over the accounts of arrested participants and staging drug buys, had successfully placed undercover agents within the inner circle of DPR's staff. This work was combined with an examination of digital traces left by Ulbricht, allowing law enforcement to triangulate his identity and the location of his server (Van Wegberg and Verburgh, 2018; Jeong, 2015). For his role in launching and operating the Silk Road website, Ulbricht was sentenced on May 29th, 2015 to life in prison without the possibility of parole (Thielman, 2015).

Whilst Operation Marco Polo represented the first major success for law enforcement, the effect in reducing the cryptomarket drug trade was short-lived. During Silk Road's operation, the marketplace had only very limited competition from three cryptomarkets created in its likeness (Digital Citizens Alliance, 2014). With Silk Road shut by authorities the two remaining cryptomarkets, Black Market Reloaded (BMR) and Sheep Marketplace, had an explosion in growth. Sheep Marketplace grew its vendor numbers by 461% within a single month after the Silk Road's closure, whilst BMR closed down citing security concerns from the increased traffic (Van Buskirk et al., 2014). Sheep Marketplace eventually was closed, but not by law enforcement efforts: following a hack of the site, the administrator closed the marketplace in a so-called 'exit scam' allowing them to abscond with user funds (O'Neill, 2015). Several new cryptomarkets emerged in their place, including "Silk Road 2.0" created by members of the old Silk Road community (Berkman, 2013a). Within four months, sales across these new markets exceeded what had been seen prior to Silk Road's closure (Soska and Christin, 2015).

2013 – 2015: The Cryptomarket Renaissance

On 6 November 2013, just over a month after the law enforcement closure of Silk Road, Silk Road 2.0 opened its doors for business under a new Dread Pirate Roberts (DPR2). Users were greeted with a homepage depicting a now-defaced FBI seizure notice reading "This Hidden Service Has Risen Again"(Greenberg, 2013). Despite the increased scrutiny that the Silk Road community was

under, DPR2 was confident in giving interviews and publicising the revival of the marketplace (Berkman, 2013b; Klippenstein, 2014). DPR2 stepped down from Silk Road 2.0 in December of the same year and nominated the user Defcon as his successor to lead the market (Mullin, 2014).

Unlike the original Silk Road, which with little significant competition dominated market share, Silk Road 2.0 faced much more competition from cryptomarkets like Evolution, Agora, Hydra and Pandora. Daily sales volume across cryptomarkets reached over USD $600,000 during the peak of this period, twice the figure Silk Road enjoyed at the height of popularity (Soska and Christin, 2015). Increased competition was reflected too in the numbers of both vendors and markets. Four months after Operation Marco Polo the number of active vendors across all markets had surpassed the 1,400 active vendors that had operated on Silk Road at the peak of its performance (Décary-Hétu & Giommoni, 2016: Soska & Christin, 2015). In 2014 alone over 40 new cryptomarkets opened, although most of them lasted less than a year (Branwen, 2018). Whilst Silk Road 2.0 was opened to much fanfare as the successor that would likely surpass Silk Road, it failed to match its predecessor in daily sales volume or vendor numbers, due to a smaller share of a highly competitive market.

Fuelling cryptomarket growth was an expansion of cryptomarket community resources on clearnet platforms. Reddit's launch of r/DarknetMarkets in 2013 created a new, popular cross-market information hub. Participants in this subreddit began creating clearnet content to support cryptomarket users, including a glossary of terms, a list of active markets, and security, buying and selling (Reddit, 2013). This was shortly followed in February 2014 by r/DarknetMarketNoobs, a subreddit catering exclusively to the needs of new users. The clearnet site DeepDotWeb was launched in 2013, and became a popular hub for cryptomarket discussion, a repository for guides on security and other topics, news-style content including details on cryptomarket-linked arrests, interviews with vendors and marketplace administrators, and user-submitted reviews. DeepDotWeb's clearnet content in support of darknet markets also provided the most comprehensive and up-to-date lists of active cryptomarkets – and critically – their (non-intuitive) .onion addresses, helping users locate the markets. It offered this content alongside its popular darknet market comparison chart, enabling site users to compare markets on key indicators of market function, including marketplace downtime, commission charged, and security features (DeepDotWeb, 2017a). These clearnet websites and discussion forums enabled regular users to keep up to date with cryptomarket developments and removed some of the knowledge barriers faced by new users in providing detailed guides to buying and selling on cryptomarkets. By providing convenient access points to otherwise hidden cryptomarkets, these clearnet resources seem likely to have played a significant role in the growth of cryptomarket trading during this period.

Alongside these clearnet informational hubs supporting the cryptomarket community, a cross-market search engine was created on the Tor network called "Grams" (Zetter, 2014). The site was modelled on Google and allowed users to search for specific vendors or products across different cryptomarkets. Grams provided additional services, including: advertising space that vendors could purchase to promote their products in search results; a bitcoin mixer called Grams Helix; and the Infodesk service that displayed top rated vendors and known scammers across markets (DeepDotWeb, 2014a). These features made Grams especially useful in the wake of a closure or exit scam by enabling users to locate vendors who had moved operations to new cryptomarkets.

An object lesson in the vulnerability of cryptomarkets and their users to law enforcement efforts, the FBI's closure of Silk Road and related arrests seems likely to have been responsible for spurring on innovations on these marketplaces, particularly in connection to security. Political discussions were popular on the original Silk Road's forum, with topics including free market

libertarianism, anarcho-capitalism, counter-economics and agorism. Research suggests that libertarian discourse on cryptomarket discussion forums dropped significantly after the closure of Silk Road (Munksgaard and Demant, 2016), suggesting that the cryptomarket community may have become less interested in political activism in favour of practical and instrumental discussion topics aimed at effective and secure market trading (Lorenzo-Dus and Di Cristofaro, 2018). There is evidence that cryptomarket users after the closure of Silk Road became more security-conscious, the PGP use for encrypted communications increased substantially (Soska and Christin, 2015), having previously often been viewed as unnecessary and additional hassle (Aldridge and Askew, 2017).

On 5-6 November 2014, six cryptomarkets were closed in a joint international law enforcement operation dubbed 'Onymous', including Silk Road 2.0. The Silk Road 2.0 administrator Defcon was revealed to be a programmer named Blake Benthall, and was arrested along with several other market administrators, vendors and staff. Authorities at first claimed that they had seized 414 different darknet websites (EuroJust, 2014), a figure later reduced to 50 (Weiser and Carvajal, 2014) and then to 27 (Vinton, 2015). Some cryptomarkets continued to operate, including the most popular marketplaces at the time, Evolution and its competitor Agora, suggesting the techniques law enforcement used were only partially effective. This seemed to be confirmed in the days that followed as a market administrator for one seized cryptomarket posted that they had evaded arrest despite their server having been seized (DeepDotWeb, 2014b).

It took some time for details to emerge concerning how law enforcement efforts had achieved multiple marketplace takedowns, and until this time, many in the cryptomarket community thought it was possible that Tor itself had been compromised, making users wary about continuing trade. In 2016 it was revealed that the attack had its roots in a technique developed by researchers at Carnergie Mellon University (CMU) to exploit Tor's infrastructure and deanonymize its users (Cox, 2016). The subpoena of CMU's research by the FBI and its role in the de-anonymisation of 78 users, including Silk Road 2.0 staff, is a matter of public record, and since this vulnerability was patched by the Tor project, no similar operations have taken place (Tor, 2016; Jerde, 2017). Whilst Onymous still relied on undercover operators and digital trace analysis, the size of the joint international effort and the exploitation of weaknesses in the technical structure of the onion-routing network to close multiple markets represented a tactical shift. Once again however, the impact of this operation was short-lived; feedback on cryptomarkets doubled from their pre-Onymous levels after only two months (Décary-Hétu and Giomonni, 2016).

This period in the evolution of drug cryptomarkets shows increasing security-related innovation and practices on marketplaces following the first exposure of cryptomarket vulnerability to law enforcement after the closure of Silk Road. In response, law enforcement operations relied more on digital knowledge and expertise in addition to more traditional undercover tactics. Despite increasing sophistication and successes in law enforcement operations, however, cryptomarket platforms remained during this period remarkably resilient; the illicit drug trade was at best briefly reduced and displaced to new marketplaces before growing again.

2015 – 2019: Toward the decentralisation of cryptomarkets?

In the wake of Operation Onymous, new cryptomarkets regularly appeared, albeit in reduced numbers. This period also saw a sharp increase in single vendor shops, typically with a specialist product focus on one or a few drug types. Although also located on the darknet, vendor shops share little in common with cryptomarkets like Silk Road and its successors that host multiple vendors and provide third party services to users in return for a commission on sales. Those

setting up single-vendor shops trade on reputations built up over time on cryptomarkets in lieu of the trust mechanisms provided by cryptomarket platforms (Persi Paoli et al., 2017).

Exit scams continued as cryptomarket administrators absconded with users' funds, sometimes generating millions of dollar in cryptocurrency for the scammers (Woolf, 2015). Discussion within the cryptomarket community suggests that users began to view exit scams as a known risk that could be mitigated by minimising funds held in cryptomarket accounts and dividing illicit trading across more than one marketplace (Reddit, 2017). Indeed, among the 78 cryptomarkets closures documented by Branwen (2018) in which the reason for closure is known, the most common (for 36 – nearly half of the marketplaces) is closure following an exit scam, vastly more common than closure due to law enforcement takedowns, confirmed by Branwen for only seven cryptomarkets. Increasing numbers of exit scams may go some way to explaining the rise in single-vendor shops since 2014, as vendors experimented with new market formations to mitigate the risk of loss selling on cryptomarket platforms in the event of an exit scam.

Cryptomarket platforms have innovated in response to the problem of exit scams by offering multi-signature escrow, in which funds from a transaction can only be released (and so become available for any use, including theft) if two of the three cryptomarket actors (that is, buyer, vendors and administrator) indicate their agreement to finalise the transaction, thereby preventing marketplace administrators having full control of funds held by the marketplace (Barratt and Aldridge, 2016). Van Buskirk et al. (2016a) found that over half of the cryptomarkets monitored between 2014 to 2016 offered an option for multi-signature escrow, suggesting that both administrators and participants saw it as a viable addition to the cryptomarket infrastructure aimed at facilitating trust in marketplaces, and therefore boosting the trade that profits both vendors and marketplace owners. Based on their corpus analysis of the *Silk Road* and *Silk Road 2* forums, Horton-Eddison and Di Cristofaro (2017) suggest that the adoption of multi-signature escrow may have been a response to law enforcement takedowns. They found that following Operation Onymous there was a marked increase in forum discussions regarding multi-signature escrow (Horton-Eddison and Di Cristofaro, 2017).

Despite the problem of exit-scams and the increase of single-vendor shops, some long-running markets such as Alphabay and Dream Market boosted user confidence as they continued to trade and grew substantially as a result. Alphabay at its peak traded over USD $600,000 per day, with its total revenue reportedly exceeding the combined revenue of all markets from 2011-2015 (Christin, 2017). Alphabay also exceeded the record set by Evolution for the highest number of vendors recorded on a cryptomarket (Van Buskirk et al., 2016a). This suggests that although the number of competing cryptomarkets reduced in the years after Operation Onymous, competition and market activity remained strong and continued to grow incrementally as strategies were devised for re-establishing user trust in cryptomarket platforms.

In 2017, coordinated law enforcement operations saw the closure of two large drug cryptomarkets: Alphabay and Hansa. The strategies used in these operations have been described in detail by Afilipoaie and Shortis (2018) and illustrate a new approach in combatting the cryptomarket drug trade: attempts to damage the trust that is essential for effective marketplace function, rather than simply closing marketplaces. In July 2017 the FBI quietly closed Alphabay without posting a seizure notice or making a public statement, having identified and arrested its alleged owner in Thailand (Swanson, 2017). Users flocked to Hansa marketplace, which reported an eight-fold increase in registrations and eventually closed registrations in order to slow the migration (Europol, 2017). Just over two weeks later it emerged that Hansa had in fact been under the control of the Dutch National Police (DNP) prior to the Alphabay closure. This meant that law enforcement had effectively and covertly continued to run Hansa by taking over as marketplace

administrators throughout the influx of former Alphabay users. The DNP changed the source code of the Hansa website to decrypt any messages sent through the sites in-built PGP system, and changed the security features of the site so that users would mistakenly download a file that would broadcast their real IP address to a DNP server. The DNP also used the login credentials they'd gained from taking over the site to change user passwords and remove bitcoins from linked cryptomarket accounts (Krebs, 2017). This multi-pronged action was followed up a year later by a second operation, in which US law enforcement agencies and the Dutch National Police, together with international partners, began a "knock-and-talk" operation on addresses they'd secured from the bust. Users were visited at their homes and warned against using cryptomarkets in future, and in some cases arrests were made (Politie, 2018).

Researchers have yet to establish if these operations have been more effective than the 'takedown' approaches used in previous law enforcement operations. Early indications based on research carried out by Van Wegberg and Verburgh (2018) shows that whilst users from Alphabay migrated to Dream Market in a similar pattern to previous takedowns, users from Hansa opted instead to change their PGP keys or usernames, suggesting they chose security over maintaining their marketplace reputations. This would suggest some success for law enforcement as their strategy was clearly designed to reduce the confidence in the cryptomarket trade rather than targeting individual sites and vendors alone. The 'honeypot' approach to the takeover of the Hansa marketplace involved sophisticated undercover operations that required highly specialised technical knowledge and skills to maintain functioning of the Hansa platform, alongside a sufficiently deep and nuanced grasp of community norms and expectations. Law enforcement officials tasked with the various roles involved in running Hansa – not just for days, but for over one month – will have needed to make decisions and communicate in writing with marketplace employees, vendors and customers all without raising suspicions in the community. However, based on monitoring carried out by the Oxford Internet Institute, Dittus (2017) found that overall cryptomarket trade volume was once again back to pre-bust levels within a month of Alphabay closing. Whilst this finding has yet to be confirmed with further peer-reviewed scholarship, it would be in line with previous recoveries to enforcement action. There is yet to be research that documents the impact of the Hansa closure that followed it, and the revelation that the site was being ran by law enforcement for the month following the closure of Alphabay.

The effect of both Operation Onymous and the Hansa and Alphabay bust was amplified by events that took place on support sites and the cryptocurrency market which led to a trend of decentralisation across several aspects of the community. Grams was shut down in December of 2017 by its administrator (DeepDotWeb, 2017b), and Reddit banned r/DarkNetMarkets in March of 2018 along with several other subreddits (Franceschi-Bicchierai, 2018). Whilst users responded by building similar platforms like the Reddit-styled hidden service *Dread*, it remains to be seen if they will be as popular. Alongside these developments, shortly after the Hansa-Alphabay bust, and not necessarily because of it, the price of bitcoin skyrocketed. The volatility led to some users preferring to keep their coins rather than engage in sales, and others were frustrated with high transaction fees and price fluctuations that left them short-changed (Lowrey, 2018). Concerns over volatility and the increasing use of blockchain analysis in investigations (Maack, 2017) led to markets offering users the option of paying for their products in Monero,[3] a more anonymous alternative to bitcoin (Torpey, 2016). These events coupled with law enforcement action have meant participants may no longer use a single forum, market or cryptocurrency in trading.

[3] At the time of writing, all popular markets listed on DeepDotWeb offer Monero as a form of payment.

Since the closure of Hansa and Alphabay, law enforcement agencies have executed operations that target the community on multiple fronts, with a renewed focus on individual participants and ancillary services that support the cryptomarket trade. The U.S. Department of Justice formed the Joint Criminal Opioid Darknet Enforcement (J-CODE) team in January of 2018 (U.S. Department of Justice, 2018b). J-CODE, a multi-agency effort to curtail the sale of drugs (particularly opioids) online, executed its first operation two months later. Operation Disarray targeted opioid customers with "knock and talk" operations aimed at deterring market participation, resulting in 160 interviews and eight arrests (U.S. Department of Justice, 2018a). Similar actions have been carried out against vendors, such as the arrest of 35 vendors in the 2018 Operation Dark Gold (U.S. Department of Justice, 2018c). Other operations have targeted support services linked to money-laundering such as the closure of the the BTC-E cryptocurrency exchange in 2017; and the BestMixer service designed to launder cryptocurrencies in 2019 (U.S. Department of Justice, 2017; Osborne, 2019). In May of 2019, DeepDotWeb, the most popular darknet news and resource site, was also closed and its owners arrested on money-laundering charges (Europol, 2019). Through targeting these support services alongside individuals, law enforcement seem to be taking a more holistic approach to cryptomarket enforcement, diminishing the ability of cryptomarket users to engage in trade through dismantling key services and resources, deterring customers and reducing the number of reputable vendors in operation

Despite these efforts, markets have persisted and events since the closure of Alphabay provide further support to research that suggests law enforcement operations are just one part of the cryptomarket threat landscape, as exit scams, denial-of-service attacks, and malicious insiders continue to pose serious threats to market stability (Aldridge and Décary-Hétu, 2016a). In March of 2019, Dream Market, the longest-running English-language cryptomarket and successor to Alphabay as market leader, announced it would be voluntarily closing following a series of denial-of-service attacks demanding ransom payments (Power, 2019). Dream's closure led to the usual migration of users to the next biggest competitor, Wall Street Market. However, in April of 2019 Wall Street Market exit-scammed, taking $11 million in user funds from the market escrow, and one of its moderators attempting to blackmail users with threats of leaking customers' delivery addresses to law enforcement (U.S. Department of U.S. Department of Justice, 2019; Cimpanu, 2019a). Days later, Wall Street Market was shut by German law enforcement, the end of a two year-long operation (U.S. Department of U.S. Department of Justice, 2019). Denial-of-service attacks resulting in market downtime frustrated the users who migrated to Empire Market and Nightmare Market (Cimpanu, 2019b). Nightmare Market also suffered a hack from within the community in July of 2019, resulting in several users being locked out of their accounts and having their funds stolen, indicating a possible exit scam (DarknetLive, 2019). These examples highlight the often chaotic environment that cryptomarkets operate within up to the present day.

What lessons then can be drawn from the evolution of cryptomarkets and law enforcement responses to them? Whilst traditional undercover operations and analysis of digital traces have been a key tactic throughout all takedown operations, the use of technical exploits in Onymous and the 'honeypot' operation that was carried out on Hansa show that policing capabilities have greatly improved. Driving these improvements are partnerships between international agencies, as well as private sector organisations that are supporting investigations with new technologies (Haan, 2018). Yet the evidence suggests that operational successes are often short-lived and motivate considerable innovations on the part of the cryptomarket community, similar to the cyclical nature of competitive adaptation between law enforcement and drug cartels in the real world (Kenney, 2007).

Whilst intergovernmental agencies have recognised that the limits of their impact on cryptomarkets and the unique challenges that they pose to law enforcement investigations, the focus of discussion has been dominated by pledges to bolster prohibitionist responses rather than

considering the consequences of these responses. At the regional level, Europol and the EMCDDA's (2017) report 'Drugs and the Darknet: Perspectives for Enforcement, Research and Policy' provides ample information about cryptomarkets and their resilience in the face of law enforcement activity, but fails to acknowledge how these activities could be driving innovation, such as increased adoption of PGP, multi-signature escrow and the adoption of more anonymous cryptocurrencies such as Monero. Similarly, at the international level, both the United Nations General Assembly Special Session on Drugs (UNGASS) Outcome Document (2016) and the World Drug Report (UNODC, 2018) discuss the need for capacity building amongst member-states in tackling drug trafficking over cryptomarkets, but remain silent on what the unintended consequences of such action might be. Considerable efforts and resources are instead focused on strengthening interdiction efforts, such as the signing of an agreement between the United Nations Postal Union and the International Narcotics Control Board to improve intelligence sharing and training for postal workers regarding drugs sent through the mail (INCB, 2018). Likewise, the EU has recently invested €5 million in funding for a project called Tools for the Investigation of Transactions in Underground Markets (TITANIUM), which aims to develop improved tools for digital forensics and blockchain analysis to help law enforcement agencies investigating cryptomarkets (TITANIUM Project, 2019). As governments and law enforcement agencies continue to apply prohibitionist approaches to this problem, a growing body of research raises questions about both the logic and the plausibility of doing so. Cryptomarkets are considerably resilient, increasingly popular and incredibly innovative, and the next section will show how they may have the potential to change the way we think about the nature, risk and harms of the global drugs trade.

Can cryptomarket drug trading transform global drug markets?

Size and scope of the cryptomarket drug trade

Researchers have documented substantial growth in the cryptomarket drug trade. Compared to annual revenue generated by Silk Road[4] of USD $15 million as measured in May 2012 (Christin, 2012), by September 2013, annual revenue only for drugs sold on the marketplace was estimated to have grown to USD $85.7 million (Aldridge and Décary-Hétu, 2014). In January 2016, drug sales across the 8 largest cryptomarkets in operation at the time had grown substantially from those generated on Silk Road just prior to its closure by the FBI. Vendors selling drugs increased from 1,084 to 5,063, drugs listed as available for sale increased from 11,904 to 105,811 and overall monthly drug revenue increased from roughly USD $7.1 million per month to USD $14.1 million per month (Aldridge and Décary-Hétu, 2014; Kruithof et al., 2016). Most commentators agree that cryptomarket drug sales represent a tiny fraction of the global trade in illegal drugs which, while impossible to estimate with any accuracy (Reuter and Greenfield, 2001) will at least be 3000 times greater. If the cryptomarket drug trade is comparatively small, why – if at all – might the online trade in drugs be an important, even transformative, development?

Features that limit the transformative potential of cryptomarkets

By taking advantage international postal services for making product shipments, cryptomarkets enable the possibility of an online drug trade that transcends international borders. This has led some commentators to suggest that these platforms could even function to link producers directly with drug-using buyers (e.g. Martin, 2014). Might cocaine producers in South America or

[4] This estimate include sales across all of Silk Road's product categories, including non-drug products and services.

heroin producers in Afghanistan use cryptomarket platforms to sell directly to drug buyers in Europe or North America? The evidence suggests that cryptomarkets are not used in this way.

Drug vendors on English-language cryptomarkets tend to be based[5] primarily in the US and Canada, Europe and Australia, with few or no vendors located where drugs like cocaine or heroin are cultivated or produced (Kruithof et al., 2016). Cryptomarkets require dependable postal and internet services and infrastructures that may not be widely and reliably available throughout countries like Colombia or Afghanistan (Martin, 2014; Demant et al., 2018). Cryptomarket vendors tend instead to be based in high-income countries with relatively high levels of illicit drug use; where, therefore, existing customer demand creates a ready market for their products. The picture that emerges from the research literature is that the cryptomarket drug trade occurs primarily in the high-income countries of the Global North. It is worth noting, however, that this research literature has so far focused on predominantly on English-language cryptomarkets; what we know about non-English language cryptomarkets trading in other jurisdictions so far is at best anecdotal.

Because of the risks entailed in making international shipments – parcel loss or interception – vendors and buyers alike may prefer making domestic transactions, and recent research suggests that domestic transactions made up an increasing proportion of cryptomarket drug transactions between 2013 and 2016 (Demant et al., 2018). Parcels shipped internationally arising from cryptomarket purchases, unsurprisingly, tend to be lower in weight than domestic-only shipments (Décary-Hétu et al., 2016). Vendors even share strategies on cryptomarket discussion forums for reducing the risks of international transactions by shipping in quantities sufficiently small to disguise as ordinary business letters (Aldridge and Askew, 2017). If international cryptomarket selling is limited to very small quantity drug transactions, the capacity for cryptomarkets to transform the structure of the global drug trade will, as a result, be limited.

Moreover, the cryptomarket drug trade caters primarily to the 'retail' trade – sales to customers likely to be making purchases for their own use, or on behalf of small friendship groups, so-called 'social supply' (Demant et al., 2016). To the extent that cryptomarkets serve a similar function to available offline retail drug markets for domestic-only trade, their transformative potential is therefore limited.

Features that facilitate the transformative potential of cryptomarkets

By bringing together multiple drug sellers on one platform, cryptomarkets make a wider range of drug types available to customers than those same customers would be able to access in their local 'offline' drug markets in face-to-face transactions with dealers. The large number of – individually often rare – psychedelic drugs available on the largest 12 cryptomarkets in January 2016: 52 separate compounds[6] were listed for sale (Décary-Hétu, personal communication) in the cryptomarket data collected for the study by Kruithof et al. (2016). Even exclusively domestic cryptomarket buying will function to expand the range of drug types available to customers beyond those in local offline markets. This is one way in which cryptomarkets may contribute to the diffusion of drugs into locales in which offline availability may be limited or non-existent.

[5] Researchers infer the geographical location of cryptomarket drug vendor operations with reference to the country from which vendors say their products will be shipped. While vendors can be based in countries other than those from which they state they will ship, these are likely to overlap substantially (Kruithof et al. 2016).

[6] These included 7 NBOMes; 11 2-c compounds; 12 other phenethylamines; 12 tryptamines and 6 lysergamides.

Cryptomarkets do not, moreover, exclusively serve the retail end of the drug trade; a – limited – 'wholesale' function is also apparent, as evidenced by the presence of high price/quantity purchases, some of whom will be customers sourcing stock for resale (Aldridge and Décary-Hétu, 2016b). Although representing only a small fraction of overall transactions, sales of drugs priced over USD $1000 (mean weight = 0.4 kilos) generate approximately one quarter of cryptomarket drug revenues (Kruithof et al., 2016; Aldridge and Décary-Hétu, 2014). Cryptomarkets may therefore operate as 'virtual brokers', linking retail and wholesale level drug market distributors (Aldridge and Décary-Hétu, 2016b). The capacity for cryptomarkets to facilitate drug diffusion may be even greater when we consider the impact that high quantity drug transactions, often advertised by vendors as ideal for 'dealers' and attracting substantial price per unit discounts (Aldridge and Décary-Hétu, 2014). Aldridge and Décary-Hétu (2016b) suggest that customers use cryptomarkets to make stock-sourcing purchases for offline distribution in local drug markets, cryptomarket-sourced drugs may ultimately serve drug takers who are not themselves cryptomarket customers.

While cryptomarkets make an exceptionally wide range of drug types available to customers, we see considerable variation in their popularity as judged by actual sales generated, as reported by Kruithof et al. (2016). Similar to the offline drug trade, sales of cannabis were dominant, and in 2016 generated 31% of all cryptomarket drug revenues. But differences to the offline drug trade were striking: ecstasy-type drugs generated many times more revenue on cryptomarkets than found in offline European drug markets. But the opposite pattern was observed for heroin, which makes up 28% of the European drugs market but only 6% of the cryptomarket trade (Kruithof et al., 2016). Returning to the wholesale function of cryptomarkets, Aldridge and Décary-Hétu (2016b) found the same drug types dominant in bulk drug selling: cannabis, MDMA and synthetic stimulants. Moreover, the vendors generating the most substantial bulk-sales revenue were often based in countries known for the production of synthetic drugs, including the Netherlands, China, Germany and Belgium (Aldridge and Décary-Hétu, 2016b). The transformative potential of drug cryptomarkets, therefore, seems likely to differ substantially by drug type. Demant et al. (2018), for example, find evidence that the cryptomarket trade may shorten supply chains for MDMA, but not for cannabis resin or cocaine, which are produced in countries in which we do not find cryptomarket vendors.

Drug price & drug quality

Emerging evidence suggests that whilst the purity of drugs on cryptomarkets can be higher when compared to offline drug sources, the prices set for them are typically higher than what most users find locally (Aldridge et al., 2018a).[7] Cryptomarket vendors, like everyone who sells drugs, must source their stock from somewhere, however the feedback mechanisms that regulate the trade may incentivise them not to adulterate their products. Analysis of 219 user-submitted cryptomarket drug samples examined by Energy Control International revealed that 90% of the samples matched the advertised content, and that the majority (64.4%) were devoid of adulterants. The purity levels for all drugs greatly exceeded samples acquired offline by the same organisation (Caudevilla et al., 2016). In a study carried out by the Dutch Drug Information Monitoring System (DIMS) which included samples from both cryptomarkets and clearnet drug stores, the differences between online and offline samples were less pronounced yet still significant for three of the nine drug categories (Van der Gouwe et al., 2016). Vendor bonds, bitcoin transaction fees, commissions paid to markets and the costs of concealing and posting the product may all be factors in explaining the relatively higher costs of cryptomarket drugs in

[7] There are some notable exceptions such as Australia, where local drug prices are significantly higher than the rest of the world (Cunliffe et al., 2017).

studies that have compared their prices to street-level drugs (Van der Gouwe et al., 2016; Economist, 2016). However, such studies have yet to adjust their reported prices for the higher purity found on cryptomarkets, and there are several reasons to think that cryptomarkets may eventually reduce prices. The wealth of information available to cryptomarket users, as well as variety of vendors and products, lower the transaction costs for customers in comparison to their offline counterparts. Given that risks are also factored in to the price suppliers charge (Caulkins and Reuter, 1998), the risk-reducing factors of cryptomarkets in lowering violence and the likelihood of detection by law enforcement may also have an impact on prices over time. Indeed evidence shows that users in Australia are likely to find ordering from vendors in other countries on cryptomarkets cheaper than local prices for specific drug types (Van Buskirk et al., 2016b; Cunliffe et al., 2017) and this might be partially explained by the higher transportation risks that street-level dealers factor into their prices (Van Buskirk et al., 2013; Cunliffe et al., 2017). It is too early to draw any conclusions at this stage based on this nascent literature, however, and further comparative research is needed that examines prices and risks for cryptomarkets and offline markets.

The potential harms and benefits of drug cryptomarkets

We have outlined some of the ways in which cryptomarkets might affect the structure of local and global markets in illicit drugs: by diffusing drugs into locations in which they were previously unavailable; by shortening supply chains; by reducing drug prices; and by increasing the likelihood that drug buyers will get the substances they pay for. But are these potential changes positive changes? Or might these changes exert negative effects? We take an evaluative approach here by assessing the harms and benefits that drug cryptomarkets may have for drug takers, drug sellers and for wider society.

Violence and conflict

Whilst cryptomarkets reduce opportunities for violence, they do not eliminate them completely. Both customers and vendors alike have reported that the lack of physical danger associated with street-level dealing has been a motivating factor in participation, and research suggests that most disputes are solved by market staff without resorting to threats or blackmail (Ormsby, 2016; Morselli et al., 2017). Comparative surveys of customers and vendors from both offline drugs markets and cryptomarkets also support these findings, showing that cryptomarket users report less threats to safety and experiences of violence as well as a reduced likelihood of detection by law enforcement in comparison to their offline counterparts (Barratt et al., 2016). Cryptomarkets have therefore been considered by some as "gentrifying" the trade in illegal drugs by physically separating participants and replacing the roles that violence plays in regulating competition and trade with digital feedback, rating and dispute systems (Martin, 2017). This normative shift goes beyond the retail level as buying in wholesale amounts removes some of the reliance on violent criminal organisations at the middle- and upper-levels of the drugs trade to source their stock (Aldridge and Décary-Hétu, 2016b). Whilst conflict may emerge in other ways that carry harms, including "doxxing" where a user's real identity is posted online (Moeller et al., 2017; Morselli et al., 2017) there is yet to be at the time of writing a recorded instance of violence carried out over a cryptomarket drug deal. Nevertheless, the potential for drug cryptomarkets to reduce violence is likely to be least effective where drug market violence is most prolific and damaging, such as producer countries of the Global South in which we see little cryptomarket activity (Demant et al., 2018). On the other hand, by bolstering demand for the drugs produced in the Global North (that is, MDMA-type drugs and cannabis), cryptomarkets may favour 'fair trade' substances over products like heroin and cocaine disproportionately associated with high levels of violence

systemic within their markets. To the extent that cryptomarkets reduce opportunities and the incidence for transactional violence, this is likely to be valued by drug buyers and sellers like, as well as be understood as a benefit in communities and for wider society.

Drug harms for users

In considering role cryptomarkets may play in reducing harms to people who use drugs, we draw here primarily on the recent detailed review of evidence by Aldridge et al. (2018a) and the response to commentaries received on the article (Aldridge et al., 2018b).

If drug takers who source their supplies on cryptomarkets are indeed likely to obtain 'as advertised' products that are less likely to be adulterated with unanticipated, unwanted or dangerous substitutes, then some of the drug harms that arise in connection to uncertain content, such as overdose, may be reduced. However, while it is likely that drug takers will value improved information about the content of their purchases, it is possible that ready availability of desired and high-quality products may increase the population prevalence in use. The wide range of products on cryptomarkets may exceed what is available to buyers in their local offline context, therefore cryptomarkets may function as a 'supply gateway' to increase population prevalence in use (Martin et al., 2018; Aldridge et al., 2018b). If cryptomarket-sourced drugs come at a lower price than similar products sourced offline, affordability may encourage new users or increase intensity of use among existing users. Similarly, drug takers who have ceased or reduced their drug use because of poor or variable quality in the drug supplies available to them offline may be motivated to restart or increase their use if they believe that cryptomarket-sourced purity will have greater certainty. More certainty around product quality may attract those motivated to take drugs who have otherwise abstained. If cryptomarkets function to increase the number of drug takers in the population, and/or increase the intensity of use for those in the population who are already users, drug harms will rise. Even if drug takers themselves value the access that cryptomarkets enable to their product of choice, any associated increases in harms are likely to be viewed as a problem by users, by others in the lives of people who use drugs, within communities, and will carry costs borne by the state in the form of drug treatment and criminal justice responses.

However, the use of illicit drugs also creates benefits for users in terms of their pleasures and functions, benefits also likely to rise alongside harms. The harms associated with increased use may be ameliorated through improved access to safer use/harm reduction information enabled on cryptomarket platforms. Whilst several clearnet forums such as Erowid and Bluelight have emerged that provide users a space to discuss safe use practices, purity and dosing, these spaces must be actively sought out by users, and discussions of sourcing may be banned to protect members and comply with increasingly strict legal requirements(Barratt, 2016; Erowid, 2001, December) . Cryptomarkets conveniently place such information at the same location as the point of sale, allowing users to discuss and feedback on the same vendors and possibly even the same stock. Therefore, we could expect any new users to have better access to harm-limiting practices shared by more experienced members of their community.

Cryptomarkets also make available a range of prescription medications (Kruithof et al., 2016). In addition to the potential risks associated with the problematic use of some of these, such as prescription opioids (Kolodny et al., 2015), medications clearly also have benefits that can be realised even for those who self-medicate, as illustrated when women residing in countries where abortion has been illegal are able to source medications to terminate their pregnancies (Aiken et

al., 2017). Cryptomarkets can also enable users of prescribed medications like opioids whose legitimate sources are curtailed by legislative changes aimed at restricting supply alternative illicit sourcing (Martin et al., 2018). Prescription opioids may be implicated in considerable harms for some users, particularly in the US, but patients in most countries across the globe face inadequate supply of these essential analgesic medications (Seya et al., 2011). Alongside prescription medications, cryptomarkets also increase the availability to drug buyers of rare/niche interest substances, particularly for a wide range of psychedelics (Aldridge and Décary-Hétu, 2016b), many of which have very low harm profiles (Elsey, 2017), some with emerging evidence for their efficacy in treating conditions of psychological ill health, such as PTSD (Tupper et al., 2015; Schenberg, 2018).

As we have seen, the scientific evidence available for assessing the potential and actual harms and benefits of drug cryptomarkets is growing, but to date remains inevitably limited given that research only began to emerge in this connection in 2012. It seems likely that the cryptomarket drug trade will reduce opportunities for transactional violence and enable people who use drugs have greater certainty around the content of their purchases, and so reduce some of the harms that arise from ingesting unknown, unwanted, or harmful substances. By enabling users to access a wider range of higher quality substances, however, the population prevalence of drug use may rise, alongside the harms associated with that use. On the other hand, the benefits associated with illicit drug use will also increase with prevalence, and some harms may be ameliorated by access to improved product quality/content and harm reduction information available to drug buyers on these marketplaces. We do not, yet, have evidence enabling us to assess potential harms against potential benefits to determine the 'net' impact. Moreover, as we have seen, cryptomarkets have evolved quickly; their impacts on net harms and benefits will therefore not remain static, as Sumnall (2018) points out.

Undertaking an evaluative assessment of harms and benefits is further complicated by recognising that what one person deems a benefit might be viewed as a harm by another. This is discussed by Aldridge (2019):

> [W]hether the potential for cryptomarkets to reduce drug harms and drug market violence is viewed as valuable depends on the perspective of the observer. If cryptomarkets indeed facilitate vendor accountability and drug buyers can therefore be more certain of the content and purity of their purchases, this is likely to be deemed valuable by drug users. Similarly, both drug buyers and vendors are likely to value marketplaces that reduce the likelihood of encountering transactional violence. In contrast, those who view the war on drugs as winnable and all illegal drug use as exclusively harm-producing, may resist casting any so-called benefits to drug users and sellers as a desirable outcome. On the contrary, any developments that benefit drug users and sellers may be interpreted as evidence of greater threat cryptomarkets pose by enabling more effective – less risky – buying and selling of dangerous illegal substances that we should be seeking to stop, rather than facilitate. Advocates of drug 'harm reduction' strategies, on the other hand, may identify any benefits of the cryptomarket drug trade as valuable. This perception may be even more likely for those who attribute much drug-related harm to drug prohibition itself – harms they believe that effective state-regulation would be better placed to reduce (Aldridge, 2019, p.582).

Conclusion

In this chapter, we have provided an explanation of cryptomarkets, including terminology and the key technologies and behaviours that support the trade, so that drug policy scholars are able to understand the virtual and anonymous context in which these markets are situated. We have shown that the evolution of cryptomarkets has been punctuated by increasingly sophisticated law enforcement operations that are basing their strategies on a deep knowledge of cryptomarket function and technologies, alongside nuanced understanding of subcultural cryptomarket community norms and expectations. Despite these efforts, cryptomarkets have continued to prosper and show resiliency to takedowns, as illustrated by the short-lived impact of operations on sales, and the consistent innovations in both security practices and the community support sites. In fact, legal action seems to pose less of a threat to a cryptomarket than the risk of the administrator stealing the funds out of their markets themselves, and therefore users have become more cautious and careful about spreading their risks across marketplaces. In the face of all these threats however, the cryptomarket community has grown significantly in the eight years it has existed, and likely will continue to do so.

Law enforcement operations have also become larger, more complex, ambitious, confident, even brazen, as illustrated when the Dutch national police took over and ran the Hansa marketplace for over a month as a honeypot. But operations of this vast scale entail substantial costs to state-funded agencies, and their successes will have been made possible through the significant investment already made by national and international law enforcement agencies in hiring new staff or upskilling existing staff (Europol and EMCDDA, 2017). This kind of heavy investment in combatting drug cryptomarkets speaks clearly about the extent to which the anonymous online trade in illegal drugs is deemed to be a serious threat. Cryptomarkets are represented as facilitating what is already deemed to be a problem (drug use and supply) in a way that threatens the ability of law enforcement and others to respond using traditional approaches. Policies and interventions aimed at combatting this threat tend not to ask important questions: does the cryptomarket drug trade produce more harms or fewer harms than generated in connection to traditional 'offline' drug markets? This is an important question to ask and answer before attempting to eradicate the online drug trade.

We assembled the available scientific evidence to shed light on how the cryptomarket drug trade might transform global drug markets. Evidence suggests that the capacity for drug cryptomarkets to transform the structure of the global drug supply is specific to particular drugs. Cryptomarket sales are dominated by ecstasy-type drugs and cannabis. These drugs are produced (synthesised or cultivated) in the same 'global north' countries in which the use of these drugs is highest and the cryptomarket drug trade is most concentrated: the US, Canada, northern and western European countries, and Australia. In contrast, cryptomarket vendors tend not to be located in producer countries for drugs like heroin and cocaine, and while these drugs are sold on cryptomarkets, it seems unlikely that cryptomarkets are likely to impact the structure of supply chains for these drugs, but instead reproduce them. By linking vendors concentrated in producer countries for cannabis and the ecstasy-type drugs directly with buyers, cryptomarkets may function to shorten their supply chains. Cryptomarkets may further function to increase drug quality and reduce purity-adjusted prices by comparison to drugs sourced in offline markets, although the evidence here is mixed.

But are these changes enabled by the cryptomarket drug trade changes for the better, or for the worse? This intentionally evaluative approach involved assessing the potential harms that may derive from cryptomarket drug sourcing against the potential benefits. Cryptomarket drug

trading may reduce transactional and systemic violence in drug markets; because drug transactions are enacted in a virtual space between relatively anonymous buyers and sellers, opportunities for violence are drastically reduced by comparison to offline drug markets, and compelling, albeit limited, research evidence supports the hypothesis that cryptomarkets may reduce violence and threats of violence. We acknowledge that cryptomarkets cannot reduce the most serious and entrenched drug market violence connected supply chains in producer countries for heroin and cocaine because cryptomarkets do not cater to these market segments. Nevertheless, cryptomarkets do serve a small but important wholesale function, particularly for ecstasy-type drugs. If violence is greater up the supply chain where purchases are made from individuals operating in organised criminal groups, and where financial stakes are higher, to the extent that cryptomarkets can serve this wholesale market level, the capacity for violence reduction there will be greater.

Regarding the effects of the cryptomarket drug trade on drug harms to people who use drugs, the picture is more equivocal. Cryptomarket-sourced drugs may be less likely than those sourced offline to contain unanticipated, unwanted or harmful substitutes or adulterants, or to be of unknown purity/strength. The harms to drug users derived from uncertain substance content such as overdose may therefore be reduced for users sourcing drugs on cryptomarkets compared to those sourcing offline. However, improved drug quality and purity available on cryptomarkets may function to increase the prevalence of drug users in the population, or increase the intensity of use of existing users, particularly if they also reduce prices. Cryptomarkets may also function as a 'supply gateway' to accessing a wider range of drugs unavailable to users in local offline markets, facilitating an expansion in drug using repertoires. They may also serve drug-motivated but previously abstaining individuals unable or unwilling to source drugs in offline markets. All these factors may increase population prevalence of drug use, intensity of use, and associated harm. Where prevalence and intensity of use increases however, harm-reducing aspects of cryptomarkets, such as the lively discussions on safe use practices and the information they offer on drug content and quality may attenuate risk. Through cryptomarkets, users can access not just drugs they want, but also drugs they might depend on for self-medication, and the growing trade in prescription opioids is a good example of the way in which harms and benefits of cryptomarkets are interconnected. Given that we are at such an early stage in the evolution of these platforms, there is a clear need for further research and comparative study designs that examine the risks and benefits of cryptomarkets in relation to offline drug markets.

There are silences in official responses in connection to the potential benefits as well as the harms of cryptomarkets. Strategies, policies and interventions that do not account for benefits in their design risk producing unanticipated and unwanted negative consequences (Aldridge, 2019). Governmental bodies and agencies alike need to consider for example where the displacement of the cryptomarket trade may lead. If trust in cryptomarkets continues to be targeted, will users decentralise further toward single-vendor shops ? These platforms use the same technology and shipping methods without any of the benefits of feedback, ratings and discussion mechanisms that help reduce harms for users. Similarly, if law enforcement effectively eradicates the less violent online drug trade back offline, will drug market violence increase? We have yet to see evidence that these questions are being considered by law enforcement agencies as they continue to pursue policies that may actually lead to increases in harms.

References

Afilipoaie, A. & Shortis, P. (2018) *Crypto-Market Enforcement - New Strategy and Tactics* [Online]. Global Drug Policy Observatory Situation Analysis. Available:

https://www.swansea.ac.uk/media/GDPOSitAnalysisJune2018AfilipoaieShortis.pdf [Accessed 20 December 2018].
Aiken, A. R., Gomperts, R. & Trussell, J. (2017) Experiences and characteristics of women seeking and completing at-home medical termination of pregnancy through online telemedicine in Ireland and Northern Ireland: a population-based analysis. *BJOG: An International Journal of Obstetrics & Gynaecology,* 124(8)**,** 1208-1215.
Aldridge, J. (2019) Does online anonymity boost illegal market trading? *Media, Culture and Society,* 41(4)**,** 578-583.
Aldridge, J. & Askew, R. (2017) Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy,* 41**,** 101-109.
Aldridge, J. & Décary-Hétu, D. (2014) *Not an 'Ebay for Drugs': The Cryptomarket "Silk Road" as a Paradigm Shifting Criminal Innovation* [Online]. SSRN. Available: http://ssrn.com/abstract=2436643 [Accessed 22 Aug 2018].
Aldridge, J. & Décary-Hétu, D. (2016a) Cryptomarkets and the future of illicit drug markets. *In:* EMCDDA (ed.) *Internet and Drug Markets, EMCDDA Insights.* Luxembourg: Publications Office of the European Union. 23-32.
Aldridge, J. & Décary-Hétu, D. (2016b) Hidden Wholesale: How drug cryptomarkets may transform traditional 'offline' drug markets. *International Journal of Drug Policy,* 35**,** 7-15.
Aldridge, J., Stevens, A. & Barratt, M. (2018a) Will growth in cryptomarket drug buying increase the harms of illicit drugs? *Addiction,* 113(5)**,** 789-796.
Aldridge, J., Stevens, A. & Barratt, M. J. (2018b) Harms, benefits and the policing of cryptomarkets: a response to commentaries. *Addiction,* 113(5)**,** 802-804.
Barratt, M. J. (2012) Silk Road: eBay for drugs. *Addiction,* 107(3)**,** 683-683.
Barratt, M. J. (2016) Bluelight.org: A harm-reduction community that supports public health research [letter to the editor]. *Journal of Substance Use,* 22(1)**,** 1-2.
Barratt, M. J. & Aldridge, J. (2016) Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy,* 35**,** 1-6.
Barratt, M. J., Ferris, J. A. & Winstock, A. A. (2016) Safer scoring? Cryptomarkets, threats to safety and interpersonal violence. *International Journal of Drug Policy,* 35**,** 24-31.
Berkman, F. (2013a) *3 Alleged Silk Road Moderators Arrested in Global Sting* [Online]. Mashable. Available: https://mashable.com/2013/12/20/fbi-silk-road-arrests/?europe=true [Accessed 10 October 2018].
Berkman, F. (2013b) *Silk Road Reborn: There's a New Dread Pirate Roberts* [Online]. Mashable. Available: https://mashable.com/2013/11/06/silk-road-dread-pirate-roberts/ [Accessed 10 October 2018].
Biderman, A. D. & Reiss Jr, A. J. (1967) On exploring the" dark figure" of crime. *The Annals of the American Academy of Political and Social Science,* 374(1)**,** 1-15.
Branwen, G. (2018) *Darknet Market Mortality Risks* [Online]. Available: https://www.gwern.net/Black-market%20survival [Accessed 21 September 2018].
Buxton, J. Bewley-Taylor, D and Hallam, C. (2017) Dealing with Synthetics: Time to Reframe the Narrative. Policy Report 6, Global Drug Policy Observatory. Available: https://www.swansea.ac.uk/media/Dealing-with-Synthetics-Time-to-Reframe-the-Narrative.pdf [Accessed 21 May 2020].
Caudevilla, F., Ventura, M., Fornís, I., Barratt, M. J., Vidal, C., lladanosa, C. G., Quintana, P., Muñoz, A. & Calzada, N. (2016) Results of an international drug testing service for cryptomarket users. *International Journal of Drug Policy,* 35**,** 38-31.
Caulkins, J. P. & Reuter, P. (1998) What price data tell us about drug markets. *Journal of Drug Issues,* 28**,** 593-612.
Chen, A. (2011) *The underground website where you can buy any drug imaginable* [Online]. Gawker. Available: http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160 [Accessed 15 August 2016].
Christin, N. (2012) *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace* [Online]. Carnegie Mellon University INI/CyLab: Technical Report CMU-

CyLab-12-018. Available: https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf [Accessed 24 April 2019].
Christin, N. (2017) *An EU-focused analysis of drug supply on the AlphaBay marketplace* [Online]. European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). Available: http://www.emcdda.europa.eu/document-library/eu-focused-analysis-drug-supply-alphabay-marketplace_en [Accessed 14 April 2019].
Cimpanu, C. (2019a) *Another dark web marketplace bites the dust --Wall Street Market* [Online]. ZDNet. Available: https://www.zdnet.com/article/another-dark-web-marketplace-bites-the-dust-wall-street-market/ [Accessed 25 July 2019].
Cimpanu, C. (2019b) *Dark web crime markets targeted by recurring DDoS attacks* [Online]. ZDNet. Available: https://www.zdnet.com/article/dark-web-crime-markets-targeted-by-recurring-ddos-attacks/ [Accessed 25 July 2019].
Cox, J. (2016) *Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds* [Online]. Motherboard. Available: https://motherboard.vice.com/en_us/article/d7yp5a/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds [Accessed 10 October 2018].
Cunliffe, J., Martin, J., Décary-Hétu, D. & Aldridge, J. (2017) An island apart? Risks and prices in the Australian cryptomarket drug trade. *International Journal of Drug Policy,* 50**,** 64-73.
DarknetLive. (2019) *Potential 'Exit Scam' Imminent After Nightmare Market Breach* [Online]. DarknetLive. Available: https://darknetlive.com/posts/nightmare-market-market-hacker-wreaks-havoc-on-the-darkweb/ [Accessed 25 July 2019].
Décary-Hétu, D. & Giommoni, L. (2016). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous, *Crime, Law and Social Change*, 67(1), 55-75.
Décary-Hétu, D., Paquet-Clouston, M. & Aldridge, J. (2016) Going international. Risk taking and the willingness to ship internationally among drug cryptomarket vendors. *International Journal of Drug Policy,* 35**,** 69-76.
DeepDotWeb. (2014a) *Grams: Becoming Hub for Darknet Info & Ads* [Online]. Internet Archive: https://web.archive.org/web/20181207232048/https://www.deepdotweb.com/2014/05/31/introducing-grams-infodesk-features-part-1/ [Accessed 25 July 2019].
DeepDotWeb. (2014b) *Multiple Market Takedown: Hydra & Cloud 9 Marketplace Seized* [Online]. Internet Archive: https://web.archive.org/web/20170606015744/https://www.deepdotweb.com/2014/11/06/multiple-market-takedown-hydra-marketplace-seized/ [Accessed 25 July 2019].
DeepDotWeb. (2017a) *Dark Net Markets Comparison Chart* [Online]. Internet Archive: https://web.archive.org/web/20190311211237/https://www.deepdotweb.com/dark-net-market-comparison-chart/ [Accessed 25 July 2019].
DeepDotWeb. (2017b) *The Darknet Search Engine 'Grams' is Shutting Down* [Online]. Internet Archive: https://web.archive.org/web/20180124070700/https://www.deepdotweb.com/2017/12/15/darknet-search-engine-grams-shutting/ [Accessed 25 July 2019].
Demant, J., Munksgaard, R., Aldridge, J. & Décary-Hétu, D. (2018) Going Local on a Global Platform: A Critical Analysis of the Transformative Potential of Cryptomarkets. *International Criminal Justice Review,* 28(3)**,** 255-274.
Demant, J. J., Munksgaard, R. & Houborg, E. (2016) Personal use, social supply or redistribution? Cryptomarket demand on Silk Road 2 and Agora. *Trends in Organized Crime,* 21(1)**,** 42-61.
Digital Citizens Alliance. (2014) *Busted, But Not Broken: The State of Silk Road and Darknet Marketplaces* [Online]. Digital Citizens Alliance. Available: https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/busted-not-broken.pdf [Accessed 19 April 2018].
Dittus, M. (2017) *A distributed resilience among darknet markets?* [Online]. Oxford Internet Institute. Available: https://www.oii.ox.ac.uk/blog/a-distributed-resilience-among-darknet-markets/ [Accessed 10 October 2018].

Economist. (2016) *Shedding Light on the Dark Web* [Online]. The Economist. Available: http://www.economist.com/news/international/21702176-drug-trade-moving-street-online-cryptomarkets-forced-compete [Accessed 20 April 2018].
Elsey, J. W. B. (2017) Psychedelic drug use in healthy individuals: A review of benefits, costs, and implications for drug policy. *Drug Science, Policy and Law,* 3**,** 1-11.
Erowid, F. (2001, December) *Web Sites with Misinformation about Illicit Drugs: A response to a letter in the New England Journal of Medicine* [Online]. Erowid Extracts 2, 12. Available: https://erowid.org/general/mentions/mentions_2001-10_nejm_response.shtml [Accessed 2 August 2019].
EuroJust. (2014) *Global Action Against Darknet Markets on Tor Network* [Online]. EuroJust. Available: http://www.eurojust.europa.eu/press/pressreleases/pages/2014/2014-11-07.aspx [Accessed 10 October 2018].
Europol. (2017) *Massive blow to criminal dark web activities after globally coordinated operation* [Online]. Europol. Available: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation [Accessed 10 October 2018].
Europol. (2019) *DeepDotWeb Shut Down: Administrators Suspected of Receiving Millions of Kickbacks from Illegal Dark Web Proceeds* [Online]. Europol. Available: https://www.europol.europa.eu/newsroom/news/deepdotweb-shut-down-administrators-suspected-of-receiving-millions-of-kickbacks-illegal-dark-web-proceeds [Accessed 25 July 2019].
Europol & EMCDDA. (2017) *Drugs and the Darknet. Perspectives for enforcement, research and policy* [Online]. Luxembourg: Europol. Available: http://www.emcdda.europa.eu/news/2017/18/darknet-report_en [Accessed 22 August 2018].
FBI. (2013) *Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website* [Online]. FBI.Gov. Available: https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website [Accessed 20 April 2018].
Franceschi-Bicchierai, L. (2018) *Reddit Bans Subreddits Dedicated to Dark Web Drug Markets and Selling Guns* [Online]. Motherboard. Available: https://motherboard.vice.com/en_us/article/ne9v5k/reddit-bans-subreddits-dark-web-drug-markets-and-guns [Accessed 10 October 2018].
Greenberg, A. (2013) *'Silk Road 2.0' Launches, Promising A Resurrected Black Market For The Dark Web* [Online]. Forbes. Available: https://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/#4818f68d5714 [Accessed 10 October 2018].
Haan, C. (2018) *Blockchain Analysis Spending by US Government Agencies Has Tripled in 2018* [Online]. Crowdfund Insider. Available: https://www.crowdfundinsider.com/2018/09/139486-blockchain-analysis-spending-by-us-government-agencies-has-tripled-in-2018/ [Accessed 10 October 2018].
Horton-Eddison, M. & Di Cristofaro, M. (2017) *Hard Interventions and Innovation in Crypto-Drug Markets: The escrow example* [Online]. Swansea: Global Drug Policy Observatory. Available: http://www.swansea.ac.uk/media/Escrow_PB11_GDPO_AUGUST2017.pdf [Accessed 20 July 2019].
INCB. (2018) *INCB/UPU act to help stem tide of trafficking in deadly synthetic opioids* [Online]. Available: https://www.incb.org/incb/en/news/press-releases/2018/signing-of-the-cooperation-agreement-between-the-universal-postal-union-and-the-international-narcotics-control-board-opening.html [Accessed 20 June 2019].
Jeong, S. (2015) *The DHS Agent Who Infiltrated Silk Road to Take Down Its Kingpin* [Online]. Forbes. Available: https://www.forbes.com/sites/sarahjeong/2015/01/14/the-dhs-

agent-who-infiltrated-silk-road-to-take-down-its-kingpin/#1182318951fb [Accessed 10 October 2018].
Jerde, R. D. (2017) *Follow the Silk Road: how Internet affordances influence and transform crime and law enforcement.* MA Security Studies Dissertation, Naval Postgraduate School, Montery, California.
Kenney, M. (2007) *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation*. Pennsylvania: Pennsylvania State University Press.
Klippenstein, K. (2014) *Dread Pirate Roberts 2.0: An interview with Silk Road's new boss* [Online]. arsTechnica. Available: https://arstechnica.com/tech-policy/2014/02/dread-pirate-roberts-2-0-an-interview-with-silk-roads-new-boss/ [Accessed 10 October 2018].
Kolodny, A., Courtwright, D. T., Hwang, C. S., Kreiner, P., Eadie, J. L., Clark, T. W. & Alexander, G. C. (2015) The Prescription Opioid and Heroin Crisis: A Public Health Approach to an Epidemic of Addiction. *Annual Review of Public Health,* 36(1)**,** 559-574.
Krebs, B. (2017) *Exclusive: Dutch Cops on Alphabay 'Refugees'* [Online]. Krebs On Security. Available: https://krebsonsecurity.com/2017/07/exclusive-dutch-cops-on-alphabay-refugees/ [Accessed 10 October 2018].
Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E. & Hoorens, S. (2016) Internet-facilitated drugs trade. An analysis of the size, scope and the role of the Netherlands. Santa Monica, RAND Europe.
Lewman, A. (2016) Tor and links with cryptomarkets. *In:* EMCDDA (ed.) *Internet and Drug Markets, EMCDDA Insights.* Luxembourg: Publications Office of the European Union.
Lorenzo-Dus, N. & Di Cristofaro, M. (2018) 'I know this whole market is based on the trust you put in me and I don't take that lightly': Trust, community and discourse in crypto-drug markets. *Discourse and Communication,* 12(6)**,** 608-626.
Lowrey, A. (2018). Bitcoin Is Falling Out of Favor on the Dark Web: The Atlantic. Available at: https://www.theatlantic.com/business/archive/2018/03/bitcoin-crash-dark-web/553190/ (Accessed: 21 May 2020)
Maack, M. M. (2017) *Danish police first in the world to hunt down criminals using bitcoin* [Online]. The Next Web. Available: https://thenextweb.com/eu/2017/02/21/danish-police-hunt-down-criminals-using-bitcoin/#.tnw_lImehQ5l [Accessed 10 October 2018].
Maddox, A., Barratt, M. J., Allen, M. & Lenton, S. (2016) Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication & Society,* 19(1)**,** 111-126.
Markoff, J. (2005) *What the Dormouse Said: How the Sixties Counterculture Sahped the Personal Computer Industry*. London: Penguin Books.
Martin, J. (2014) *Drugs on the dark net: how cryptomarkets are transforming the global trade in illicit drugs*. Basingstoke: Palgrave Macmillan.
Martin, J. (2017) Cryptomarkets, systemic violence and the 'gentrification hypothesis'. *Addiction,* 113(5)**,** 797-798.
Martin, J., Cunliffe, J., Décary-Hétu, D. & Aldridge, J. (2018) Effect of restricting the legal supply of prescription opioids on buying through online illicit marketplaces: interrupted time series analysis. *BMJ,* 361.
Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M. & Savage, S. (Year) A fistful of bitcoins: characterizing payments among men with no names. *In:* Proceedings of the 2013 conference on Internet measurement conference, 2013. ACM, Barcelona, Spain. 127-140.
Moeller, K., Munksgaard, R. & Demant, J. (2017) Flow My FE the Vendor Said: Exploring Violent and Fraudulent Resource Exchanges on Cryptomarkets for Illicit Drugs. *American Behavioral Scientist,* 61(11)**,** 1-24.
MoneroHow. (2017) *How does Monero privacy work?* [Online]. Monero.how. Available: https://www.monero.how/how-does-monero-privacy-work [Accessed 10 October 2018].

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M. & Aldridge, J. (2017) Conflict Management in Illicit Drug Cryptomarkets. *International Criminal Justice Review,* 27(4)**,** 237-254.
Mullin, J. (2014) *Silk Road 2.0, infiltrated from the start, sold $8M per month in drugs* [Online]. arsTechnica. Available: https://arstechnica.com/tech-policy/2014/11/silk-road-2-0-infiltrated-from-the-start-sold-8m-per-month-in-drugs/ [Accessed 10 October 2018].
Munksgaard, R. & Demant, J. (2016) Mixing politics and crime–The prevalence and decline of political discourse on the cryptomarket. *International Journal of Drug Policy,* 35**,** 77-83.
Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System* [Online]. Bitcoin.org. Available: https://bitcoin.org/bitcoin.pdf [Accessed 20 April 2018].
O'Neill, P. H. (2015) *Suspected Dark Net master thief busted trying to buy luxury Czech home* [Online]. The Daily Dot. Available: https://www.dailydot.com/crime/sheep-marketplace-scam-arrested/ [Accessed 22 August 2018].
Ormsby, E. (2016) Silk Road: insights from interviews with users and vendors. *In:* EMCDDA (ed.) *Internet and Drug Markets, EMCDDA Insights.* Luxembourg: Publications Office of the European Union.
Osborne, C. (2019) *Bestmixer seized by police for washing $200 million in tainted cryptocurrency clean* [Online]. ZDNet. Available: https://www.zdnet.com/article/bestmixer-seized-by-eu-police-over-laundering-of-200-million-in-cryptocurrency/ [Accessed 25 July 2019].
OSF. (2011) *War on Drugs: Report of the Global Drug Commission on Drug Policy* [Online]. Open Society Foundation (OSF). Available: https://www.globalcommissionondrugs.org/wp-content/themes/gcdp_v1/pdf/Global_Commission_Report_English.pdf [Accessed 20 August 2018].
Persi Paoli, G., Aldridge, J., Ryan, N. & Warnes, R. (2017) Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web. Santa Monica, Calif., and Cambridge, UK: RAND Corporation.
Politie. (2018) *Operation Mirum, Darkweb is Not Anonymous* [Online]. Dutch National Police. Available: https://www.politie.nl/nieuws/2018/februari/15/operation-mirum-darkweb-is-not-anonymous.html [Accessed 10 October 2018].
Power, M. (2019) *The World's Biggest Dark Net Market Has Shut – What Next?* [Online]. VICE. Available: https://www.vice.com/en_uk/article/wjmw3w/dark-web-net-dream-market-closed-theories [Accessed 25 July 2019].
Reddit. (2013) *Reddit r/DarknetMarkets (now closed)* [Online]. Internet Archive. Available: https://web.archive.org/web/20131201050416/http://www.reddit.com/r/DarkNetMarkets/ [Accessed 22 August 2018].
Reddit. (2017) *DNM Buyer Bible: 6.1 - Important Tips for Using Markets* [Online]. Archive.Today. Available: https://archive.is/yo4oF [Accessed 10 October 2018].
Reuter, P. & Greenfield, V. (2001) Measuring global drug markets. *World Economics,* 2(4)**,** 159-173.
Schenberg, E. E. (2018) Psychedelic-Assisted Psychotherapy: A Paradigm Shift in Psychiatric Research and Development. *Frontiers in Pharmacology,* 9(733)**,** 1-11.
Seya, M.-J., Gelders, S. F., Achara, O. U., Milani, B. & Scholten, W. K. (2011) A first comparison between the consumption of and the need for opioid analgesics at country, regional, and global levels. *Journal of pain & palliative care pharmacotherapy,* 25(1)**,** 6-18.
Soska, K. & Christin, N. (2015) Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *In:* Proceedings of the 24th USENIX Security Symposium (USENIX Security '15), 12-14 August 2015, Washington DC. 33-48.
Sumnall, H. R. (2018) The harm reduction impact of cryptomarkets; inequality and opportunity. *Addiction,* 113(5)**,** 801-802.
Swanson, K. (2017) *Suspected AlphaBay founder dies in Bangkok jail after shutdown of online black market* [Online]. Washington Post. Available: https://www.washingtonpost.com/news/morning-mix/wp/2017/07/18/suspected-alphabay-founder-dies-in-bangkok-jail-while-online-black-market-remains-closed/?utm_term=.c7e0eee6673e [Accessed 10 October 2018].

Thielman, S. (2015) *Silk Road operator Ross Ulbricht sentenced to life in prison* [Online]. Guardian. Available: https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced [Accessed 10 October 2018].

TITANIUM Project. (2019) *TITANIUM: Tools for the Investigation of Transactions in Underground Markets* [Online]. Available: https://titanium-project.eu [Accessed 20 June 2019].

Tor. (2016) *Statement from the Tor Project re: the Court's February 23 Order in U.S. v. Farrell* [Online]. Tor Project. Available: https://blog.torproject.org/statement-tor-project-re-courts-february-23-order-us-v-farrell [Accessed 10 October 2018].

Torpey, K. (2016) *Darknet Customers Are Demanding Bitcoin Alternative Monero* [Online]. Bitcoin Magazine. Available: https://bitcoinmagazine.com/articles/darknet-customers-are-demanding-bitcoin-alternative-monero-1472243603/ [Accessed 10 October 2018].

Tupper, K. W., Wood, E., Yensen, R. & Johnson, M. (2015) Psychedelic medicine: a re-emerging therapeutic paradigm. *Canadian Medical Association Journal,* 187(14)**,** 1054-1059.

U.S. Department of Justice. (2017) *Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox* [Online]. U.S. Department of Justice. Available: https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged [Accessed 25 July 2019].

U.S. Department of Justice. (2018a) *Attorney General Jeff Sessions Announces Results of J-Code's First Law Enforcement Operation Targeting Opioid Trafficking on the Darknet* [Online]. U.S. Department of Justice. Available: https://www.justice.gov/opa/pr/attorney-general-jeff-sessions-announces-results-j-code-s-first-law-enforcement-operation [Accessed 25 July 2019].

U.S. Department of Justice. (2018b) *Attorney General Sessions Announces New Tool to Fight Online Drug Trafficking* [Online]. U.S. Department of Justice. Available: https://www.justice.gov/opa/pr/attorney-general-sessions-announces-new-tool-fight-online-drug-trafficking [Accessed 25 July 2019].

U.S. Department of Justice. (2018c) *First Nationwide Undercover Operation Targeting Darknet Vendors Results in Arrests of More Than 35 Individuals Selling Illicit Goods and the Seizure of Weapons, Drugs and More Than $23.6 Million* [Online]. U.S. Department of Justice. Available: https://www.justice.gov/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35 [Accessed 25 July 2019].

U.S. Department of Justice. (2019) *3 Germans Who Allegedly Operated Dark Web Marketplace with Over 1 Million Users Face U.S. Narcotics and Money Laundering Charges* [Online]. U.S. Department of Justice. Available: https://www.justice.gov/usao-cdca/pr/3-germans-who-allegedly-operated-dark-web-marketplace-over-1-million-users-face-us [Accessed 25 July 2019].

UNODC. (2016) *Outcome Document of the 2016 United Nations General Assembly Special Session on the World Drug Problem* [Online]. United Nations General Assembly Special Session on the World Drug Problem. Available: http://www.unodc.org/documents/postungass2016//outcome/V1603301-E.pdf [Accessed 20 April 2019].

UNODC. (2018) *World Drug Report 2018*. Vienna: United Nations Office on Drugs and Crime.

Van Buskirk, J., Naicker, S., Bruno, R., Burns, L., Breen, C. & Roxburgh, A. (2016a) *Drugs and the Internet, Issue 7, October 2016* [Online]. Sydney: National Drug and Alcohol Research Centre. Available: https://ndarc.med.unsw.edu.au/sites/default/files/ndarc/resources/dnetbulletin_issue7_final.pdf [Accessed 20 May 2019]

Van Buskirk, J., Naicker, S., Roxburgh, A., Bruno, R. & Burns, L. (2016b) Who Sells What? Country Specific Differences in Substance Availability on the Agora Dark Net Marketplace. *International Journal of Drug Policy*. 35, 16-23.

Van Buskirk, J., Roxburgh, A., Bruno, R. & Burns, L. (2013) *Drugs and the Internet, Issue 1, August 2013* [Online]. Sydney: National Drug and Alcohol Research Centre. Available:

https://ndarc.med.unsw.edu.au/sites/default/files/ndarc/resources/DrugsTheInternet_Newsletter%20FINAL%20with%20ISSN.pdf [Accessed 20 May 2019].
Van Buskirk, J., Roxburgh, A., Farrell, M. & Burns, L. (2014) The closure of the Silk Road: what has this meant for online drug trading? *Addiction,* 109(4)**,** 517-518.
Van der Gouwe, D., Brunt, T. M., van Laar, M. & van der Pol, P. (2016) Purity, adulteration and price of drugs bought online versus offline in the Netherlands. *Addiction,* 112(4)**,** 640-648.
Van Hout, M. C. & Bingham, T. (2013) 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy,* 24(5)**,** 385-391.
Van Wegberg, R. & Verburgh, T. (2018) Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market. *In:* Evolution of the Darknet Workshop: 10th ACM Conference on Web Science (WebSci '18). 27-30 May 2018. Amsterdam, Netherlands.
Vinton, K. (2015) *So Far Feds Have Only Confirmed Seizing 27 "Dark Market" Sites in Operation Onymous* [Online]. Forbes. Available: https://www.forbes.com/sites/katevinton/2014/11/07/operation-onymous-dark-markets/ [Accessed 10 October 2018].
Wagner, A. (2014) *The Role and Future of Altcoins* [Online]. Bitcoin Magazine. Available: https://bitcoinmagazine.com/articles/role-future-altcoins-1400813009/ [Accessed 10 October 2018].
Weiser, B. & Carvajal, D. (2014) *International Raids Target Sites Selling Contraband on the 'Dark Web'* [Online]. New York Times. Available: https://www.nytimes.com/2014/11/08/world/europe/dark-market-websites-operation-onymous.html?_r=0 [Accessed 10 October 2018].
Woolf, N. (2015) *Bitcoin 'Exit Scam': Deep-Web Market Operators Disappear With $12m* [Online]. London: Guardian. Available: http://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars [Accessed 1 April 2019].
Zetter, K. (2014) *New 'Google' for the Dark Web Makes Buying Dope and Guns Easy* [Online]. Wired. Available: https://www.wired.com/2014/04/grams-search-engine-dark-web/ [Accessed 10 October 2018].
Zimmermann, P. R. (1995) *The Official PGP User's Guide*. Cambridge MA: MIT Press.