Article

Producing Trust Among Illicit Actors: A Techno-Social Approach to an Online Illicit Market

Angus Bancroft
University of Edinburgh, UK

Tim Squirrell
University of Edinburgh, UK

Andreas Zaunseder
University of Aberdeen, UK

Irene Rafanell
University of the West of Scotland, UK

Abstract

Illicit market exchanges in cybercriminal markets are plagued by problems of verifiability and enforceability: trust is one way to ensure reliable exchange. It is fragile and hard to establish. One way to do that is to use the administrative structure of the digital market to control transactions. This is common among a specific type of market – darknet cryptomarkets. These are sites for the sale of illicit goods and services, hosted anonymously using the Tor darknet. However, reliance by users on the technology and the market administrators exposes users to excessive risk. We examine a case of a market that rejects several key technological features now common in cryptomarkets but that is nonetheless reliable and robust. We apply a techno-social approach that looks at the way participants use and combine technologies with trust relationships. The study was designed to capture the interactional context of the illicit market. We aimed to examine both person-to-person interaction and the technical infrastructure the market relied on. We find that the social space of the market maintains itself through a shared common security orientation, community participation in key decisions about products sold, performing trust signalling, and relying on lateral trust between members. There are implications for how resilience in cryptomarkets is understood.

Corresponding author:

Angus Bancroft, Sociology Department, The University of Edinburgh, 18 Buccleuch Place, 4.05, Edinburgh EH8 9JS, UK.
Email: angus.bancroft@ed.ac.uk

Introduction

Trust has been called a part of the deep structure of social life (Lewis and Weigert, 1985) and a response to the risk inherent in cooperation with others (Luhmann, 2000). It is thought to depend on characteristics of social closeness and institutional robustness. Relationships conducted online present a challenge for maintaining trust. Trustful actors can be impersonated and trust signals faked to little cost for the malicious actor. That is particularly important for online illicit market exchanges, where there is a strong incentive to falsify and where the cost of doing so is low and the sanctions limited. Licit online markets and social media tend to substitute technical features such as likes, followership, and reviews for the workings of interpersonal trust. This is difficult for participants in illicit online markets, who need to disguise their identities and where there is no incentive to stick to agreements. Yet these markets operate robustly and even embed moral sanctioning within them (Masson and Bancroft, 2018). There is a strong emphasis on technical and cultural competence with illicit markets which is attained through a combination of mutual sanctioning and avoidance of technological fixes to problems of communication and anonymisation. Trust is then moved from a problem of quality assessment and transactional reliability to one of relational embedding (Beckert and Wehinger, 2012). This article is about the balance between technical features of illicit online communities, their social embedding, and the paradox whereby more technically 'sparse' settings can lead to more reliable interactions. The article takes one critical case, that of a darknet illicit drug market forum we have dubbed 'PsychForum market' (PFM).

The solution to the trust paradox is thought to lie either technically in the use of reputation mechanisms in open online markets specifically designed for the purpose, exemplified by darknet cryptomarkets (Barratt and Aldridge, 2016; Martin, 2014), or relationally in contractual agreements in closed, private markets (Van Wegberg et al., 2018). In these closed markets, trust signalling performance is necessary to be recognised as a legitimate actor (Gambetta, 1988). In the cryptomarkets there is a high turnover of vendors and buyers, so direct trust signalling is less effective. Community evaluations of participants are more significant, and most markets have a discussion forum where vendors and buyers participate. To be involved successfully participants must be skilled at interpreting the signals and traces made by others (Décary-Hétu and Leppänen, 2016).

Cryptomarkets are typically hosted using the Tor darknet. Tor allows for anonymised hosting where users and hosts cannot easily be located. Payments can be made via the bitcoin cryptocurrency payment system which allows for a degree of anonymity when used for this purpose. Encryption underlies these technologies. The Pretty Good Privacy (PGP) encryption standard allows for closed communication over otherwise open networks. Cryptomarkets appear as shopfronts, with lists of products for sale (Aldridge and Décary-Hétu, 2014), typically a range of illicit drugs and other illegal electronic services (Afilipoaie and Shortis, 2015). The administrators regulate what can be sold on the market and take a cut of sales. The cryptomarkets mediate the 'last mile' of the drug trade, the part

of the supply chain going from wholesalers to dealers (Aldridge and Décary-Hétu, 2016) and to a lesser extent from dealers to consumers (Demant et al., 2018; Dittus et al., 2017). Further distribution then takes place in person or through social media (Moyle et al., 2019). They allow dealers and buyers to solve coordination problems common to illicit markets (Bakken et al., 2018; Beckert and Dewey, 2017). They are relatively resilient in the face of disruption from law enforcement and rivals (Van Buskirk et al., 2017), partly due to the technical features of the darknet and also because of economically rational and ideological commitments from users (Ladegaard, 2017).

Those entering the markets must find ways to manage risks. The markets themselves usually offer third-party dispute resolution (Morselli et al., 2017). Such systems, however, have shown themselves to be technically robust but socially brittle. Vendors who have previously been known as trustworthy have disappeared overnight, taking their customers' money with them. Mostly, trust is build up through a commitment to repeat purchase (Décary-Hétu and Quessy-Doré, 2017). The growing threats from both law enforcement and hostile actors have shifted the market power structure away from consumers and towards vendors, so more powerful vendors can use the system to push risk back onto the consumer (Moeller et al., 2017). As well as altering the economic and social structure of the drug market they have an impact on normative interaction, promoting both prosocial displays (Martin, 2017) and a 'rational consumer' stance by participants (Barratt et al., 2016b). In comparison, we explore a system of building and maintaining trust that is technically unsophisticated but socially resilient, in which users have a shared commitment to the market as a community. PFM has outlasted many apparently more technically better designed or financially successful markets. It eschews centralised technical features such as reputation systems and centralised payment clearance, and it has minimal price or advert-based trust signalling, yet it undoubtedly works well. This indicates that some technical and interpersonal features of illicit online markets that are held by their user communities to be central to their success are neither necessary nor sufficient conditions for them to work. In practice, they require a committed, culturally integrated community to function (Dodd, 2018). Key to PFM's function is its cultural performance and signification in which technical competence and personal identity are articulated together to create a common interactional space. The article shows the process of performance and contestation that an illicit online market uses to produce trust.

Context and methodology

The study was designed to capture the interactional context of an illicit market. We aimed to examine both interactions and the technical infrastructure of the market (Stratton et al., 2017). We observed how cryptomarket users interacted with each other and how these interactions contributed to social sanctioning and the creation of shared norms and agreements in the market. We captured changes over time in the market and observed the dynamics of knowledge production and evaluation that we hypothesised were central to the market processes working effectively. We took an ethnographic approach involving five months of observation of interactions in PFM in the second half of 2017. This was a time when morale in the cryptomarket ecosystem was at a low ebb (Ladegaard, 2018). Two major markets were closed down by law enforcement (LE) and one was subject to an exit scam.

Initial themes were written up from the observations. We copied the forum text into a database and coded the textual data in the light of the initial themes. We then returned to the market for a further observation period in order to check the coding themes and note how PFM had responded to internal and external changes. External changes consisted of the collapse of other cryptomarkets during this period due to scams and LE-led shutdowns. Internal changes came in response to an influx of new users and proposals to adopt new drugs for sale. In response to the large number of new users, the administrators closed registrations for a time, as the numbers were too great to permit any kind of security checking process. During the data collection phase, the team also observed other discussion forums, such as Reddit threads, dedicated to cryptomarkets in order to track changes in PFM against the wider cryptomarket ecosystem.

PFM was selected as a case because its design emphasises the centrality of interaction and the users' assessment of whom to trust, when, and to what extent. It is a hybrid of a discussion forum and a market focused on community-approved psychedelic drugs. Two characteristics of our case are significant. First, PFM does not offer centralised, integrated secure payment such as escrow or auto-encryption functions commonly emblematic of cryptomarkets. Instead, users personally contact vendors through manually PGP-encrypted private messages. Second, the administrators and key users of the PFM specifically restrict the kinds of drugs which can be advertised to a select set of psychedelics – consciousness-altering drugs typically used for self-exploration. This latter feature was crucial for us. It means that there is continual contestation and engagement over which drugs are sold and which are proscribed.

Ethical approval was obtained from the School of Social and Political Science ethics review committee. The PFM administrators were contacted initially in order to make them aware of the research project, but no return contact was established. In order to protect what is a fragile ecosystem and the privacy expectations of users, we have pseudonymised and also obfuscated text-based quotes and usernames in order to prevent identification. Cryptomarkets are of interest to LE as a growing area of illicit activity that appears to be both openly accessible and beyond the reach of traditional investigation methods. As the location of both the markets and their users is uncertain, it is unclear what legal and normative frameworks govern research into them. Martin and Christin (2016) develop the ethical domains defined by Whiteman (2012) in online research. *The ethics of the academy* are the commonly held claims and norms governing ethics in research. Some aspects of this domain are grounded in preexisting understandings about the distinction between public and private, and it is often assumed that this is a simple and consistent distinction which researchers can respect. However, in online research there may be varied norms and assumptions at work. Researchers may treat as public conversations those which the participants assume are private. Observing PFM participants it was apparent that there was a generalised awareness that the discussions were open and not private, so it was considered ethical to make use of this data. The *ethics of the researcher* is the disciplinary and personal stance adopted by researchers towards the field. We take the view that cryptomarkets are illegal but self-governing and largely not directly harm producing, and should be taken seriously as communities of practice which regulate their members. Therefore we take the view that research should contribute to showing the range of behaviours and personae within PFM and also accept that moral and prosocial activity can be part of cryptomarket interaction. That leads us into the *ethics of the researched* and their personal motivations
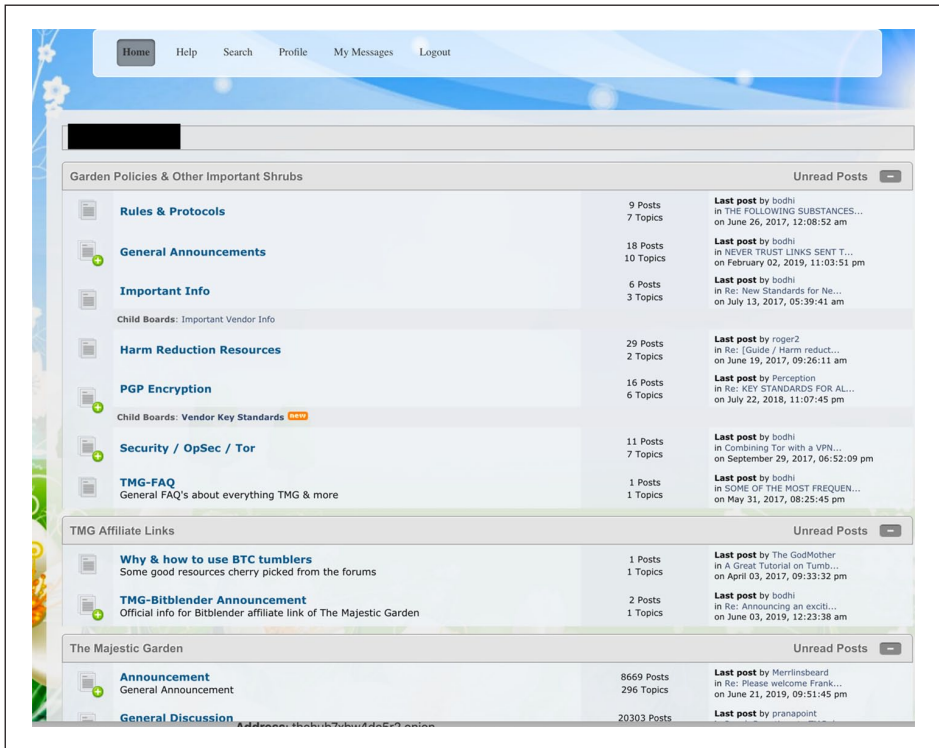
Figure 1. PFM's landing page.

and boundaries. We noted that maintaining PFM as a coherent, effective entity was important to the participants as was spreading the gospel of psychedelic drug experience. Their ethics included respecting privacy and taking responsibility for personal security. To a large extent that meshed with our approach. Finally the *ethics of the institution* present a challenge. British universities promote high-impact research, and that tends to be framed in research that serves the interests and priorities of public institutions. Our approach is informed by tenets of sociology and addresses a range of publics, including communities that are considered to be deviant or lawbreaking. There has been extensive discussion about whether cryptomarkets can reduce or increase drug harms (Barratt et al., 2016a, 2016b; Mounteney et al., 2018). Researchers should not make any a priori assumption as to what effect they have and therefore what 'side' we should take. We can use our methods to elaborate on the motives and experiences of cryptomarket users and put the impact of cryptomarkets on the drug trade and drug use culture in context.

Findings: the market forum as a status group

PFM has the appearance of a basic Internet discussion forum. It consists of a large number of discussion threads, has few adornments, and carries no adverts (Figure 1). This presentation is part of the general approach of the market. It operates as a bounded collective, a

Figure 2. PFM discussion threads.

grouping of individuals who share a particular life-style, a distinctive psychedelic culture, and idiosyncratic notions of social esteem and honour. It emphasises the responsibility of each participant for their own security and safety, and their obligation to the community. PFM is maintained by a small grouping of administrators who also emphasise that they will not take responsibility for losses or errors by users. The main focus of discussion is psyche-delic drugs and drug experiences, but users also post extensively on other topics, such as the state of the darknet, drug politics, philosophy, other markets, and bitcoin (Figure 2).

Threads focus on the reliability of different drug vendors, the products for sale, scientific knowledge and personal experiences with specific types of drugs, debates around personal security – called 'operational security' or opsec–and harm reduction. There is no immediate distinction between vendors and buyers. Other cryptomarkets allow buyers to rate vendor performance. Instead of vendor ratings, all PFM members are rated by status markers which are linked to expectations and restrictions on the behaviour of group members. These are the quantity of their contributions to forum threads, symbolic feedback in the form of compliments and reports embodied in 'Karma', awards (e.g. 'Wizard' or 'Connoisseurs Club'), and status markers such as 'Elder' or 'Newbie'. Such group status markers are indicators of the shared common stock of knowledge and accepted practices which constitute this particular group

culture as a shared life-world. We argue that trustworthiness is one such marker in the PFM community, both influencing and emerging as a product of interaction between users: administrators/moderators, vendors, and other members. Maintaining this sense of a flat organisational system is vital to ensuring that participants do not rely on the market administrators for the market to function:

> Why I came here in the first place was the reviews of sellers and drugs which folk were uploading. I enjoy that the forum is like a distributed governing agency which completely has everyone's backs covered. The forest grew from a bunch of sound folks' aim to develop the purity of the drugs we all love so much, and while doing so supporting and nurturing the users of said drugs. It is the reason for me being into hallucinogenic before I discovered the internet. You need people who have an eye for quality and for the risks people are in, who can put that before money. So awesome to see there's this global group targeted on taking liability, avoiding risks, being in good spirits about it and telling everyone who needs to know. Big thumbs up! (Forum user, Wastis)

In contrast to more centralised cryptomarkets, the PFM ethos encourages problems to be resolved through discussions between buyers and vendors. Users understand that they are buying into this approach when they join the market:

> I at the moment have shown up due to not getting what I ordered last month from [Vendor] to MidWest USA. It was just a few stickers of LSD. I expect it'll be sorted between us, I've taken my time as we're in holiday mode. I messaged the vendor a few days past, radio silence for now. I'll hold back and have another go on this place and the vendor's own message board. (Forum user, Finetime)

Lines of communication are kept open between administrators and users during times of crisis in order to maintain the fabric of trust that sustains the capacity of PFM to fulfil its role as a forum and space to purchase drugs. When PFM was subject to multiple distributed denial of service (DDOS, a form of electronic attack) attacks, the administrators moved the market to another host until they were able to bring the site back up as we noted in the Reddit discussion. Given the intrinsically precarious and potentially compromised nature of cryptomarkets, one might ask why anybody would trust a darknet forum enough to interact with other individuals and potentially purchase illicit drugs through it. In this first section, we will explore how individual users relate to the idea of trusting the forum and its administrators, as well as how those administrators along with experienced users and vendors discuss and enforce opsec norms upon new users.

Enforcing a common security orientation

PFM users noted that reliance on centralised trust-promoting technology such as escrow payment systems and market-based encryption services created significant risks of compromise by LE. They eschewed some of this technology in favour of embedded personal relationships and a shared orientation to security. An administrator welcome post exhorts how new users ought to both use and treat the forum:

> Number one, the main point: educate yourselves about the risks you are taking.

Never show your true ID, other than when one to one with a seller who you have checked out
No open internet data like social media or gmail

Encrypt everything.

This places the burden upon the buyer to induct themselves with respect to the vendors from whom they purchase and the various security measures that they ought to implement. They are expected to possess or acquire skills in using encryption for communication (e.g. generating a public and private PGP key). There are numerous links to those measures, including how-tos for PGP encryption and bitcoin tumbling (a form of money laundering). The administration team took the decision to enforce a rule that all private messages must be manually encrypted, rather than encrypted automatically by the market's own system as is typical of other cryptomarkets, and to ban users who repeatedly flout this rule as otherwise 'again and again it is clear everyone defaults to the easy path instead of the secure one'. The admin references the recent registration shutdown, saying,

Should ourselves let the market be accessible then the community has to be an unsafe space for the police should they get into and take it over … all crypto places should have taken steps like that in the time after the Silk Road [the first cryptomarket] was seized.

The encryption mandate is backed up by rhetoric that asks users to act as though the forum is already compromised, putting no trust whatsoever in those who run it to keep them safe if they were to make any mistakes: 'Work under the knowledge that LE is targeting PFM and it is best to act as if it has already been taken over by them. Act like that when dealing with everything on the darknet'.

The act of telling users not to trust blindly paradoxically demonstrates trust in the community. It demonstrates a care for users that goes beyond the functional. There is a degree of community solidarity, rooted in a common feeling of marginalisation and repression, both as a result of the war on drugs at large and the specific context of recent LE crackdowns. This contrasts with more predatory criminal forums, where those who get caught tend to be written off as simply bad or careless criminals. This is the kind of sympathy that is displayed by the same Reddit user quoted above, who states, 'I doubt anyone likes it when LE takes its victories even when they are up against idiots. Better the idiots than LE!'. Solidarity emerges as a function of the kind of community that the administrators try to create, which prioritises harm reduction and risk mitigation. It is also pragmatically necessary for the community to work. It is simply bad business to have one's customers arrested, and the downfall of a vendor has the potential to poison the whole community.

The forum design is meant to winnow out higher-risk users in three ways. The first is through a dedicated 'Newbie Corner' with a 50-post minimum before users can go onto the main forum described as 'the filter through which we can isolate and filter would be scammers, annoyances, and shams. Newbie corner helps make PFM work smoothly and nicely for everyone'. Users confirm,

Rules like the 50 post one usually wind me up but truth be told it works and I'm partial to it. It gives this place the sense that it's a shared space, I can find out who I can Interact with and rely

on, and it lets me get a feel for the people on here. Even when it's Tor, you should know your neighbourhood.

The quality of engagement of members and their contribution to the community (e.g. the helpfulness of their contributions, and helping out) can be evaluated and acknowledged – individually through Karma points, and more comprehensively through awards (e.g. 'Awesome Contributor', 'Quickest Responses' or 'Critical Update Provider').

The second is to make the space unfriendly to occasional retail users who may be less capable and less skilled. In contrast to more commodified cryptomarkets which attempt to render the process of signing up and purchasing drugs as simple as possible, PFM forces new users to learn the ropes. It provides the resources for them to do so, but the administrators straightforwardly refuse to do the work for them. In the long run this may be safer than retail markets which let users sink or swim. A further impact is that administrators, vendors, and ordinary users are better able to trust users who have remained and made purchases, safe in the knowledge that they are likely to have educated themselves in opsec.

The third is to restrict the intake of new users. A PGP-signed message from a forum moderator was posted after registrations had been reopened following a long closure:

> So we can manage and limit the flood of recent intakes, there will be case by case confirmation of newbies by the administrators. We are doing that to ensure that you are all encrypting things properly and maintaining the rules that are there for everyone's wellbeing.

In this instance we see that they are prepared to compromise short-term membership gains and potential revenue in order to secure the site against both hacking and LE incursion. In the words of the most prominent advocate for opsec in the forum community, when asked whether there could possibly be exceptions for the encrypted private messages rule:

> Don't be daft, ENCRYPT FROM BEGINNING TO END. No DISCUSSION on this front. A simple message on the open internet has been enough to land some folks in prison.

Trust performance and negotiation

Trust is cultivated, mediated, performed, and negotiated between vendors, users, and administrators. PFM has no escrow system, meaning that buyers are expected to pay before the product is shipped to them. That should mean that buyers are taking on a very high risk as there is little incentive for the vendor to deliver as promised. However, the system appears to work well. PFM places heavy emphasis upon the diligent scrutiny of vendor applications by the administrators as well as upon the importance of user reviews of vendors. It also means that vendors act as if they are obligated to PFM as a whole to produce the drugs as promised. So there is a working mutual obligation that is not underpinned by any technical system in place. It is largely driven by word-of-mouth reputation.

A non-escrow model puts the buyer at risk of 'selective scamming' from the seller (a practice where vendors will fail to ship, say, 1/100 items and keep the money, with no possibility of it being verified as a scam rather than law enforcement confiscating the package or it

getting lost in the post). However, it also protects users from the possibility of an exit scam, where the marketplace owner steals all of the money in escrow and users' wallets in a certain period. One way of framing this issue is that escrow-based cryptomarkets require users to trust the market owner not to run away with a lot of money, whereas non-escrow models only require users to trust vendors not to run away with a much smaller amount of money (while losing all possibility of operating as a vendor again). Users note that the reputation system on cryptomarkets is easily gamed and that the reviews posted on this forum are a better indicator of quality: 'Fantastic the way that we buy straight from vendors and keep them honest without any nonsense salesforce advertising and reputation fluffing. Three times I have been exit scammed or markets have disappeared. Better to be one on one with a vendor.'

This closer relationship means buyers enjoy having contact with vendors. One says, It's enjoyable gassing with sellers. I'll be more relaxed when making a purchase and it means they might get a bit extra from me – like a good Uber drive. We both come out on top.' Others wish to observe vendors' interactions with other buyers, so that they can 'make it so sellers that are doing business with me are ones that give a nod to their buyer's health and safety as well as their profit margins'. This user cares not only about the quality of the product but also about the way vendors treat their customers and whether they 'appreciate that the drugs they are selling can make people's lives better'. Many users want 'have a one to one bond with buyers we can rely on so the substances we buy are dependable and quality'.

That generates a positive feedback loop. Users are quick to praise vendors whom they deem to have gone above and beyond in the service they have provided. One user recounts an experience they have had with OmegaOgre, a large vendor of psychedelics:

> While ago I bought from OO but didn't heard anything. After a lot of confusion when I finally got communicating with him, RIGHT AWAY he gave me the option of my money back or the goods, at his own expense. And I had made so many mistakes in going about things the right way. You are my top seller, you give me delight and drugs and I want everyone to know.

The vendor–buyer relationship is mediated by the forum administrators. There are sections of the forum dedicated to 'rogue vendors', who are now blacklisted as a result of having scammed users, providing poor quality product, or disappearing for significant periods of time. Moderators on the forum willingly mediate complaints between users and vendors, particularly when those complaints become numerous. In one notable instance, the administrators made a public announcement that 'Following much thought and reflection, based on what we know and what's been passed to us, with some reluctance we post this warning for anyone who has bought from Suicide Squad'. The post says they 'take this action with sadness' but wish to prioritise the 'security of the forum and everyone who might have exchanged with them'.

The post goes on: 'We have to take it as read that the team have been compromised. We cannot just casually think that it will all be fine or that it is an accident without a backup in place'. The trust that was once present can never be regained. ' There is no way of him demonstrating that he isn't under heavy manners to anyone's satisfaction. There's no evidence he could offer.?' asks the moderator. They conclude that 'we have together outlawed everyone in that team, none of them can participate in the forum now.' The banning of all of the vendor's team partly functions to protect the community from LE, who may have control of

their accounts, but it also serves to close the door on the incident. There is no coming back from this loss of trust.

There are lingering questions in the community about how to deal with the potential for vendors to be compromised by LE at any time. In much the same way as the administration team was forced to 'assume the worst' in the case of Team Honesty, senior community members argue that there is no real way to 'take care to select your seller with caution and common sense. They aren't always what they seem. Act as if every one of them is clueless and is unable to maintain their own security.' Reviews tell users nothing about vendors' internal security arrangements. The only time it becomes apparent that a vendor's opsec was lacking is after the fact, when they are arrested, and even then it is unclear for just how long they were compromised.

One user argues that

> Bigger and more established do not imply more reliable and trustworthy. Over and over we have found that those who say they are secure are not. The longer you are on the darknet, the bigger you get, there's more interest from LE and more time for things to go wrong and the longer the trail you leave for them to pick up.

Longevity gives no indication that a vendor is doing things properly and might indicate that the vendor is at increased risk of downfall.

At the same time, there is very little reason that users would purchase from vendors who were not established, and it appears that the only way that they would be willing to do so would be with the endorsement of comparatively known quantities. One user states, 'The only reason I would have to start with a new vendor we don't know about would be if they were vouchsafed by a well known one'. They go on,

> What it comes down to is your money is going to a stranger, and you have to take a risk with them if you purchase drugs on the darknet. That puts your safety in their paws.

Likewise, the administrators have struggled to negotiate the changing environment of the cryptomarkets, where fewer dependable cryptomarkets up and running means that fewer vendors are able to establish themselves as reputable. This shows how the cryptomarkets work as a connected market ecosystem rather than a series of disparate unconnected platforms. Reputation on one is crucial to reputation on another. Not having its own reputation system made PFM dependent on the wider cryptomarket system. One administrator complains,

> There is no way a seller can demonstrate their chops unless they are well ensconced here. The reason is that to apply the vendor has to have been on for most of a year and have a large numbers of reviews elsewhere. It becomes more difficult to demonstrate that record when many cryptomarkets are offline.

While PFM acts as a refuge it still relies upon other cryptomarkets as means of acquiring new vendors. The only way around this, for the administrators, is to defer to the judgement of those they already trust:

There is a way by which sellers can start themselves off. A top seller can put in a word for them,
the upshot is that the top seller has to cover any costs that the new vendor incurs so new vendors
can start.

Contested knowledge problems

One way in which users invest in the PFM community is through participating in inten-
sive discussions on what drugs can be sold through it. One poster describes the birth of
the PFM (as forum) and the people who created it:

The PFM site in fact is the creation of a bunch of folks who started in the Silk Road. At that time
the psychedelic market in the darknet was wall to wall crooks. Team PFM began with testing
drugs being sold as LSD. They showed up crooks and validated honest, dependable sellers.
Doing that meant that the cryptomarkets could be places where LSD could be sold honestly and
reputably.

We can examine one controversy to demonstrate the way that trust in and respect
for the administrators are invoked as a means of enforcing rules and setting bounda-
ries for the drug trade. PFM declares that drugs sold must broadly have low addiction
and harm potential and significant use for self-exploration. They permit cannabis,
LSD, MDMA, psilocybin, and DMT. Specifically banned are 'Spice and other artifi-
cial cannabis types, speed and associated analogues, GHB and anything you might
expect: cocaine, Oxycontin, crystal meth and the like'. The banned drugs include a
range of drugs commonly associated with problems of addiction, overdose, and
harmful behaviour. For example, GHB is often characterised as a drug that facilitates
sexual assault.

A live controversy revolves around ketamine. There have been significant issues with
ketamine access, with 'an American shortage of Ketamine which has sent prices up three
times over the decade'. Additionally, 'ketamine can't really be replaced [substituted by
the user]' as opposed to many other substances that are difficult to acquire but have sub-
stitutes readily available. In August 2017, a user created a 'petition to add ketamine to list
of approved substances'. The moderators' stance was that

there are no future plans to approve Ket for sale due to its potential for causing dependence. The
continuous use of it creates health risks which we know well. We are not going to allow it or be
part of it.there are no future plans to approve Ket for sale due to its potential for causing
dependence. The continuous use of it creates health risks which we know well. We are not
going to allow it or be part of it.

The poster responds that 'there are other substances on sale here which could be as
dependence inducing at Ket' and 'a single dependable seller could fix the K shortage and
also limit the number of phony and cut drugs being sold'.

An administrator weighs in:

Take a small town and hand a thousand folk ten grams of K each. What proportion would show
dependence, how many might OD, or use it to sexually assault people? Most people in PFM
would not misuse it however we cannot let these sales happen.

The root of the controversy in this instance appears to be that members trust this forum over and above any other and so are upset that they are unable to source what they consider to be an important and useful drug there. One member asks, 'Do any forums on the darknet permit K to be bought and discussed? Reddit's rules now make it difficult and shady and the cryptomarkets are full of scammers or useless'.

The reason the administrators refuse to compromise on their principles is not just to avoid the potential attention that would be drawn by allowing ketamine dealers on to their site, and nor is it simply a matter of concern for addictive potential. Instead, it can be accounted for by the need for the administrators to be seen to be consistent and to maintain the integrity of the forum as a space where only certain kinds of activities are facilitated and condoned. These negotiations of what can be sold on PFM serve a harm reduction purpose and demonstrate users' personal investment.

Discussion

The illicit economy is closely intertwined with the formal economy, and changes in both go tougher closely. The illicit drug economy introduced a Fordist, low-skill criminal economy into the world during the 1980s (Ruggiero, 2001). Divisions of labour grew, and roles were deskilled and more easily entered into or abandoned. Whereas crime service producers were one the major players in the illicit economy, now criminal service consumers are (Ruggiero and South, 1997). Likewise digital criminal activity was for a time dominated by the work of skilled actors embedded in hacker communities (Steinmetz, 2015). The emergence of online illicit markets means that their participants can be less technically skilled and work in less densely networked and more disperse groups (Aldridge and Décary-Hétu, 2016). Indeed the bulk of online illicit drug transactions take place through location apps, websites, and social media, in what are highly technically insecure environments (Bakken and Demant, 2019; Moyle et al., 2019). This presents risks for participants as it exposes them to relatively easy compromise. PFM addresses these challenges by mutual oversight of members.

The kind of trust PFM exemplifies is a lateral relation, exemplified by solidarity and recognition of common interest, rather than a vertical reliance on administrators and owners that other markets attempt to inculcate. Participants have a shared commitment to the idea of PFM as a purposeful community. Members justified their activity by demonstrating how they took more care for people's health and psychological well-being than straight society and other cryptomarkets. Trust was a quality articulated by the moral community of PFM, and it underlay their expressed ideology and the choices they made about what was sold and why. The relationship between the discussion forum and the market function is an essential aspect for its success. PFM emphasised trust taking place within a bounded community of those interested in psychedelics. Larger markets with a more laissez-faire policy to products for sale are not likely to have the inbuilt community support that this one did.

Users favourably compare their experience on PFM to other communities they have found on the clearnet. They locate that difference in quality of experience in two specific aspects. First, they care about the capacity to source drugs. Presumably the reason that they enjoy participating in this community in addition to buying drugs, rather

than simply buying here and talking elsewhere, is because they see some value to the combination of the two. We posit that trust in product and vendors is in part a function of trust in the other people who also purchase that product or from those vendors. Second, they locate the difference in culture in the different kinds of drugs sold on this forum. Their objection to opioids is partly ethical, but they also see communities that sell these drugs as being 'hostile' and 'giving drug users a bad name'. This echoes the discussion around ketamine where administrators and users alike were wary of the impacts selling it might have upon the constitution of the community itself.

In other threads, users engage in discussions about topics as banal as what they ate that day and as profound as what it means to experience 'ego death' while tripping on LSD. There is personal disclosure from people on the forum who find it a place where they can relax and talk about the things that matter to them without fear of judgement or legal trouble, and with the certainty that there are other people who share their interests. The community thrives not just because of the pragmatic concern that users should trust the people reviewing the people who are going to sell them illicit mind-altering substances. It thrives because there are bonds of interdependence being formed between like-minded people who feel as though they are not completely at home elsewhere, even in other places where drugs can be bought and sold.

PFM participants replaced trust in personal relationships and trust in technology with a hybrid of reputation and know-how. Moving away from relying on centralised escrow and PGP could show that some of these technologies were more used as performances of trust and theatre of security rather than because they actually provided reliable service. For example, scams are built into vendors and buyers' cost calculations. 'Don't trust the tech' is part of a geek orientation to technology. In stating that one relies on one's own assembly of the technology, one shows one's agency and how the user is in charge of the technology rather than the other way around.

Participants relied on their personal encryption methods as PFM did not run its own because reliance on the cryptomarkets' own technology exposes users to risk. In the event of the markets' systems being compromised, all users are potentially exposed and this was what compromised users of Alphabay, Hansa, and other markets (Afilipoaie and Shortis, 2018). So this tells us about how market actors respond to threats and what makes particular markets more or less resilient than others. It also tells us what law enforcement priorities are, and that some markets may survive by being insignificant or diffuse enough to be more trouble than they are worth. LE takedowns tend to make use of darknet and blockchain analysis technology to investigate markets and assume that users place the same value on the technology they do, but this may be incorrect.

In the PFM community the acquisition of 'trustworthiness' is a key status marker of the group. This develops the insight of Luhmann (2000) that norms and values of a particular community define the boundaries of its membership and define what is to count as trust and who is trustworthy. We take this insight further because mistrust is not just negation of trust. Rather it is a fundamental building block of the generation of trust in this specific environment. The generalised mistrust imposed by the forum administrators and adopted by all participants of the forum becomes key to group formation and underpins the conception of trust which operates in this collective. It is one which becomes a

'collective good' and acting as a status marker of 'belonging' to this particular collective (Barnes, 1992). It is a collective good which is key not only to group formation but to the internal organisation of inter-individual interactions and group dynamics.

Conclusion

LE strategies have tended to focus on the affordances of technology as the driving force in cybercrime (European Union, 2017). We have illustrated a case where users' shared understanding of the purpose of the market and the carefully self-imposed limits of the technology they use are key to the stability and security of their market. This techno-social approach has implications for how we understand the combination of criminal motivations, technology, and community that forms each online illicit market. Users' cultural competence is central to their ability to navigate the market and the signals that they send to others regarding their trustworthiness. Additionally, this organisational arrangement is used to govern what drugs are sold and for what purpose and makes PFM a place where drugs are discursively constructed as either part of the community or harmful to it.

References

Afilipoaie A and Shortis P (2015) *From Dealer to Doorstep – How Drugs Are Sold on the Dark Net*. Swansea: Global Drug Policy Observatory.

Afilipoaie A and Shortis P (2018) *Crypto-Market Enforcement – New Strategy and Tactics*. Swansea: Global Drug Policy Observatory.

Aldridge J and Décary-Hétu D (2014) *Not an 'e-bay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation*. Rochester, NY: Social Science Research Network.

Aldridge J and Décary-Hétu D (2016) Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy* 35: 7–15.

Bakken SA and Demant JJ (2019) Sellers' risk perceptions in public and private social media drug markets. *International Journal of Drug Policy*. Epub ahead of print 1 May. DOI: 10.1016/j. drugpo.2019.03.009.

Bakken SA, Moeller K and Sandberg S (2018) Coordination problems in cryptomarkets: Changes in cooperation, competition and valuation. *European Journal of Criminology* 15(4): 442–460.

Barnes B (1992) Status groups and collective action. *Sociology* 26(2): 259–270.

Barratt MJ and 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 MJ, Ferris JA and Winstock AR (2016b) Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy* 35: 24–31.

Barratt MJ, Lenton S, Maddox A, et al. (2016a) 'What if you live on top of a bakery and you like cakes?' Drug use and harm trajectories before, during and after the emergence of silk road. *International Journal of Drug Policy* 35: 50–57.

Beckert J and Dewey M (2017) Introduction: The social organization of illegal markets. In: Beckert J and Dewey M (eds) *The Architecture of Illegal Markets: Towards an Economic Sociology of Illegality in the Economy*. Oxford: Oxford University Press, pp. 1–34.

Beckert J and Wehinger F (2012) In the shadow: Illegal markets and economic sociology. *Socio-Economic Review* 11: 5–30.

Décary-Hétu D and Leppänen A (2016) Criminals and signals: An assessment of criminal performance in the carding underworld. *Security Journal* 29(3): 442–460.

Décary-Hétu D and Quessy-Doré O (2017) Are repeat buyers in cryptomarkets loyal customers? Repeat business between dyads of cryptomarket vendors and users. *American Behavioral Scientist* 61(11): 1341–1357.

Demant J, Munksgaard R and Houborg E (2018) Personal use, social supply or redistribution? cryptomarket demand on Silk Road 2 and Agora. *Trends in Organized Crime* 21(1): 42–61.

Dittus M, Wright J and Graham M (2017) Platform criminalism: The 'last-mile' geography of the Darknet market supply chain (arXiv:1712.10068 [cs]). Available at: http://arxiv.org/abs/1712.10068

Dodd N (2018) The social life of Bitcoin. *Theory, Culture & Society* 35(3): 35–56.

European Union (2017) *Serious and Organised Crime Threat Assessment 2017*. The Hague: European Police Office.

Gambetta D (1988) Can we trust trust? In: Gambetta D (ed.) *Trust: Making and Breaking Cooperative Relations*. Oxford: Basil Blackwell, pp. 213–237.

Ladegaard I (2017) 'I pray that we will find a way to carry on this dream': How a law enforcement crackdown united an online community. *Critical Sociology* 45: 631–646.

Ladegaard I (2018) We know where you are, what you are doing and we will catch you: Testing deterrence theory in digital drug markets. *The British Journal of Criminology* 58(2): 414–433.

Lewis JD and Weigert A (1985) Trust as a social reality. *Social Forces* 63(4): 967–985.

Luhmann N (2000) Familiarity, confidence, trust: Problems and alternatives. In: Gambetta D (ed.) *Trust: Making and Breaking Cooperative Relations*. New York, NY: B. Blackwell, pp. 94–107.

Martin J (2014) *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs*. London: Palgrave Macmillan.

Martin J (2017) Cryptomarkets, systemic violence and the 'gentrification hypothesis'. *Addiction* 113: 797–804.

Martin J and Christin N (2016) Ethics in cryptomarket research. *International Journal of Drug Policy* 35: 84–91.

Masson K and Bancroft A (2018) 'Nice people doing shady things': Drugs and the morality of exchange in the darknet cryptomarkets. *International Journal of Drug Policy* 58: 78–84.

Moeller K, Munksgaard R and Demant J (2017) Flow my FE the vendor said: Exploring violent and fraudulent resource exchanges on cryptomarkets for illicit drugs. *American Behavioral Scientist* 61: 1427–1450.

Morselli C, Décary-Hétu D, Paquet-Clouston M, et al. (2017) Conflict management in illicit drug cryptomarkets. *International Criminal Justice Review* 27: 237–254.

Mounteney J, Cunningham A, Groshkova T, et al. (2018) Looking to the future-more concern than optimism that cryptomarkets will reduce drug-related harms. *Addiction* 113: 799–800.

Moyle L, Childs A, Coomber R, et al. (2019) #Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy* 63: 101–110.

Ruggiero V (2001) *Crime and Markets: Essays in Anti-Criminology*. Oxford: Oxford University Press.

Ruggiero V and South N (1997) The late-modern city as a bazaar: Drug markets, illegal enterprise and the 'barricades'. *The British Journal of Sociology* 48(1): 54–70.

Steinmetz KF (2015) Craft(y)ness an ethnographic study of hacking. *The British Journal of Criminology* 55(1): 125–145.

Stratton G, Powell A and Cameron R (2017) Crime and justice in digital society: Towards a 'digital criminology'? *International Journal for Crime, Justice and Social Democracy* 6(2): 17–33.

Van Buskirk J, Bruno R, Dobbins T, et al. (2017) The recovery of online drug markets following law enforcement and other disruptions. *Drug and Alcohol Dependence* 173: 159–162.

Van Wegberg R, Tajalizadehkhoob S, Soska K, et al. (2018) Plug and prey? Measuring the commoditization of cybercrime via online anonymous markets. In: *Proceedings of the 27th USENIX conference on security symposium*, Baltimore, MD, 15–17 August.

Whiteman N (2012) *Undoing Ethics: Rethinking Practice in Online Research*. New York: Springer.

Author biographies

Angus Bancroft is a lecturer in Sociology at the University of Edinburgh. He researches cryptomarkets, illicit markets in drugs and other goods and services which use the Tor darknet, alcohol consumption cultures, and smart drugs.

Tim Squirrell is a PhD student in the Department of Science, Technology, and Innovation Studies at the University of Edinburgh. He has worked as a research assistant on two projects in the School of Social and Political Science: the Carnegie-funded 'Theorising Cybercriminals' project under Angus Bancroft and the ESRC-funded EMoTICON project under Julie Brownlie. His doctoral research focuses on the construction and negotiation of authority and expertise in online self-improvement communities, exploring how users relate to concepts of evidence and credibility on the social news site Reddit. He has engaged in independent research and freelance journalism on the subject of online extremist communities, including the alt-right and 'incel' communities. He currently works as the senior course tutor in two introductory Sociology modules and has also taught on Social Policy courses.

Andreas Zaunseder is a PhD candidate at the Centre for Citizenship, Civil Society, and Rule of Law at the University of Aberdeen. For several years, he has worked as tutor and senior tutor in Sociology and Sustainable Development as well as research assistant in Sociology at the University of Edinburgh. Andreas is a cofounder of the interdisciplinary research network 'World of Work', which spans several universities across the UK. He currently serves as editor at *H-Citizenship*. His doctoral research investigates the political culture of workers' cooperatives in Scotland. He has been involved as co-investigator in research projects on cryptomarkets (in the darknet) and the grassroots politics of alternative gatherings and festivals.

Irene Rafanell is a Sociology lecturer at the University of the West of Scotland and an Honorary Fellow of the School of Social and Political Studies at Edinburgh University. Her research focuses on articulating new analytical and methodological premises bringing together theoretical tenets from social constructionism, sociology of knowledge, and sociology of the body.